The Data Center Anarchists' Handbook

A Public Interest Guide to Data Center Development

The Data Center Anarchists' Handbook by Lawrence Nault is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**.

This handbook is a public-interest resource. It is not legal, engineering, environmental, financial, or regulatory advice. Readers should consult qualified local experts, Indigenous governments, public authorities, and applicable laws before relying on it in a specific project or jurisdiction.

You may copy, share, quote, adapt, translate, and redistribute this work, including for commercial purposes, provided you give appropriate credit, indicate whether changes were made, and release adaptations under the same licence.

DOI: **10.5281/zenodo.20645367**

Introduction

This handbook is not an argument against data centers.

Data centers are now part of the infrastructure of modern life. They support communication, research, commerce, public services, artificial intelligence, cloud storage, health systems, education, entertainment, and countless other parts of daily life.

The question is not whether data centers should exist.

The question is whether they should be approved, subsidized, connected, powered, cooled, and built before governments, communities, and the public have the tools to properly understand their impacts.

This handbook is a response to the rapid, seemingly unimpeded expansion of data center development across towns, counties, provinces, states, nations, watersheds, farms, forests, and communities. Too often, approvals move faster than the laws, methods, protocols, monitoring systems, and public safeguards needed to govern them. Too often, the conversation begins with promises of investment, jobs, innovation, and economic growth, while the harder questions are delayed, softened, fragmented, or left unanswered.

Those harder questions matter.

They matter because data centers are not just buildings filled with servers. They are industrial-scale demands on electricity, water, land, cooling systems, transmission infrastructure, tax policy, emergency planning, noise regulation, and public trust. They can affect people, communities, animals, plants, waterways, farmland, air quality, local economies, and entire ecosystems. They can reshape land-use decisions, public budgets, energy planning, water security, Indigenous rights, municipal services, and the future obligations left to residents long after the ribbon-cutting is over.

It is painfully clear to me that, as an author, I spend far too much time researching.

As someone who writes about systems, the environment, artificial intelligence, technology, public policy, and the strange places where all of those things collide, I tend to collect questions. Notes upon notes upon notes. Fragments of research. Policy ideas. Environmental concerns.

Technical explanations. Warnings from one sector that seem to echo in another. Observations that begin as background for fiction and eventually become too relevant to leave buried in a notebook.

The Data Center Anarchists' Handbook began as something much smaller.

Originally, the concept was intended to appear as an addendum in a future book in ***The Symbiosis Sequence***, my conceptual science-fiction series exploring technology, humanity, artificial intelligence, and the systems we build before we fully understand them. In that fictional context, it was going to be called *The AI Anarchists' Handbook*. It was not supposed to be this long. It was not supposed to become a public document. It was meant to be a sharp, fictional artifact — a small set of questions embedded in a larger story about power, technology, and consequence.

Then the real world kept catching up.

Recent news, public proposals, data center announcements, government enthusiasm, industry language, infrastructure pressure, and the speed of approvals made it increasingly difficult to keep these questions tucked away for a future novel. The issue was no longer only useful as fiction. It was happening now, in real communities, with real water, real electricity, real land, real public money, real farms, real neighbours, real ecosystems, and real consequences.

So this handbook became something else.

It became a place to put many of the questions I keep asking.

That is important: this handbook does not provide the answers.

It is not a technical manual. It is not a legal opinion. It is not an engineering assessment. It is not a regulatory submission. It is not a substitute for local expertise, Indigenous governance, public consultation, environmental review, municipal planning, utility analysis, or legal advice.

It is a handbook of questions.

There are no references in these pages by design. That may seem unusual, especially for a document built from research, but the choice is intentional. Information changes quickly. Laws change. Projects change. Technologies change. Cooling systems change. AI workloads change. Utility agreements change. Water conditions change. Ownership structures change. Public claims change. What is current today may be incomplete tomorrow.

Instead of pretending this handbook can freeze a fast-moving issue in place, it gives readers a framework for inquiry.

If you can ask the questions in this book, you can take the next step and research why they should be asked. You can ask your council. You can ask the developer. You can ask the utility. You can ask the regulator. You can ask for the studies. You can ask for the agreements. You can ask for the monitoring data. You can ask for the public cost. You can ask what has been left out.

The goal is not to replace research.

The goal is to make research possible.

This handbook was created as a tool. It was designed by an author who has spent far too much time studying, researching, questioning, and considering the impacts of uncontrolled

development — not as an engineer, industry consultant, lobbyist, or elected official, but as a citizen, writer, and observer trying to understand what communities are being asked to accept.

It does not contain every question. No handbook could. It also does not assume that every question in these pages should be asked in every situation. A small facility, a hyperscale campus, a publicly owned research installation, a private AI training center, a rural development, an urban retrofit, and a data center proposed in a drought-prone watershed do not all raise the same concerns.

Instead, this is a handbook of questions we should be willing to ask before, during, and after the approval process.

Before approval, because communities deserve to know what is being proposed before decisions become difficult to reverse.

During approval, because public hearings, consultations, environmental reviews, utility agreements, water licences, tax arrangements, and zoning decisions should be informed by more than promotional language.

After approval, because accountability does not end when construction begins, when servers go live, or when the first tax incentive is granted.

The purpose of this handbook is not to tell communities what conclusion to reach. It is to help them ask better questions. It is to give residents, journalists, councillors, landowners, Indigenous governments, public officials, environmental advocates, workers, farmers, parents, students, and neighbours a starting point for scrutiny.

Some readers may come to these questions because they are worried about water. Others because they are worried about electricity. Others because they are worried about noise, farmland, public subsidies, Indigenous rights, foreign ownership, privacy, artificial intelligence, wildlife, taxes, emergency services, or the basic democratic problem of decisions being made before the public has enough information to understand them.

All of those entry points matter.

A data center is not one issue. It is many issues gathered inside one fence.

That is why the questions have to be gathered too.

A community cannot meaningfully consent to what it has not been allowed to understand.

And if data centers are going to become part of our shared future, then the public must have the right, the language, and the tools to ask what that future will cost — and who will be expected to pay for it.

A Note on Finding Authority

This handbook does not cite sources. That choice is explained above: the facts move too quickly to freeze in a footnote, and what is accurate in one place may not apply in another.

But not citing sources is not the same as telling readers to trust no one.

The questions in this handbook are starting points. The answers live elsewhere — in institutions, records, and research that already exist, and that the public has a right to consult. When a question

in these pages matters to you, the next step is to find the body, document, or study that can answer it for your situation.

Several kinds of authority are worth seeking out.

Your utility regulator or energy board governs electricity rates, grid connections, and who pays for new transmission. They often hold the power agreements and cost studies the public never sees in a council presentation.

Your water licensing or watershed authority controls how much water can be withdrawn, from where, and under what conditions. They hold the licences, the limits, and the drought rules.

Your environmental review or assessment agency sets the threshold for what must be studied before approval, and holds the assessments once they exist.

Your municipal or local planning office holds the zoning, the site plans, the expansion rights, and the conditions of approval.

Your emergency services and public health authorities can speak to response capacity, fire risk, and the burden a facility places on local responders.

Beyond government, two further categories matter.

Peer-reviewed studies — published research subjected to independent expert scrutiny — are the strongest available evidence on questions of water use, emissions, noise, health, and ecological impact. A single study is not proof, but a body of peer-reviewed work is far more reliable than a developer's brochure or a single expert's assurance.

Fact-checked, independent journalism can document what has happened at comparable facilities elsewhere: the promises made, the promises kept, the disputes, the costs, and the consequences other communities have already lived through. Favour reporting that names its sources and corrects its errors over coverage that simply repeats announcements.

No single authority holds the whole picture. That is part of the problem this handbook describes. But together, these bodies and sources are where the real answers are kept.

If you can ask the question, you can find who is supposed to answer it.

And if no one can — if the regulator has not studied it, the agency has no record of it, and no independent research or reporting exists — that absence is itself an answer worth bringing to a public hearing.

A Note on Language

This handbook uses words drawn from one country's system: *council* and *councillor*, *province*, *municipality*, *Indigenous governments*, *water licence*.

Your jurisdiction may use others.

A *council* may be a county board, a commission, a local authority, or a planning department. A *province* may be a state, a region, a prefecture, or a department. A *utility regulator* may be a public utilities commission, an energy board, or a national grid authority. The body that governs water, land, environmental review, or public consultation will carry a different name almost everywhere.

The names change. The questions do not.

Wherever you are, the task is the same: find the body that holds the power to decide, the document that records the decision, and the public's right to see both.

A Note on Structure and Repetition

This handbook is built on a deliberately repeated structure.

Most chapters follow the same pattern: a plain-language explanation of the issue, a set of core questions, a list of red flags, a summary of what communities should ask for, and a public-interest standard. This repetition is intentional. It is meant to make the handbook easier to use.

Few readers will read this document from beginning to end. Most will arrive because of a single concern — water, electricity, noise, taxes, data, emergency planning — and turn directly to the chapter that addresses it. A consistent structure means a reader can open any chapter and immediately know where to find the questions, the warning signs, and the documents to request, without having read the chapters before it.

For the same reason, some information appears more than once.

A concern raised about water may also matter for electricity, cooling, emergency planning, and cumulative impact. Rather than send readers backward through chapters they may not have read, this handbook restates what is relevant where it is relevant. A point that matters in five places is made in five places.

This is a reference tool, not a narrative. It is meant to be opened to the page you need.

Contents

Introduction 1

A Note on Finding Authority 3
A Note on Language 4
A Note on Structure and Repetition 5

Part One: Before the Approval 1

1 - What Is Actually Being Proposed? 1

The Problem With Vague Proposals 1
Facility Type 2
Scale 2
Purpose 3
Owner 3
Operator 4
Tenants and End Users 4
Timeline 5
Expansion Rights 5
Single Facility or Larger Campus? 5
Existing Infrastructure Capacity 6
The Importance of Plain Language 6
Core Questions 7
Facility Type 7
Scale 7
Purpose 8
Owner 8
Operator 8
Tenants and Users 8
Timeline 9
Expansion Rights 9
Campus or Single Facility 9
Existing Infrastructure 10
Public Understanding 10
Red Flags 10
What Communities Should Ask For 11
The Public Interest Standard 11

2 - Who Benefits? 13

Public Benefit Versus Private Gain 13
Who Receives the Money? 14
Land Value and Speculation 14

Jobs as Benefit 15
Tax Revenue as Benefit 15
Infrastructure as Benefit 16
Digital Access as Benefit 16
Community Benefit Versus Community Branding 17
Who Carries the Burden? 17
Distribution of Benefits 18
Time Matters 18
Core Questions 18
Financial Benefit 18
Public Benefit 19
Jobs 19
Tax Revenue 19
Infrastructure Benefit 19
Digital Access 20
Community Benefits 20
Burdens 20
Timing 21
Red Flags 21
What Communities Should Ask For 21
The Public Interest Standard 22
3 - Who Decides? 23
The Approval Map 23
Municipal and Local Authority 24
Provincial or State Authority 24
Federal Authority 25
Utility Regulators and Grid Authorities 25
Water Licensing Bodies 25
Environmental Authorities 26
Indigenous Governments and Rights-Holders 26
Zoning Boards, Planning Commissions, and Appeals 27
Public Consultation Rules 27
Public Agencies as Customers 28
The Problem of "Not Our Jurisdiction" 28
Core Questions 29

Approval Process 29
Municipal and Local Authority 29
Provincial or State Authority 29
Federal Authority 30
Utility and Grid Decisions 30
Water Decisions 30
Environmental Review 30
Indigenous Governments 31
Zoning and Planning 31
Public Consultation 31
Government Roles 31
Accountability 32
Red Flags 32
What Communities Should Ask For 32
The Public Interest Standard 33
4 - Public Consent and Consultation 35
Consultation Before Commitment 35
Information Must Be Complete Enough to Respond 36
Plain Language 36
Access to Documents 36
Notice Must Reach the Affected Public 37
Accessibility 37
Consultation Is Not Advertising 37
The Right to Ask Follow-Up Questions 38
Meaningful Hearings 38
The Problem of Pre-Approval Momentum 38
Consent and Indigenous Rights 39
Consultation With Those Most Affected 39
Consultation Records 39
Public Consent Is Ongoing 39
Core Questions 40
Timing 40
Information Provided 40
Documents 40

Notice 41
Accessibility 41
Hearings 41
Consultation Quality 42
Indigenous Governments 42
Most Affected Communities 42
Ongoing Consent 42
Red Flags 43
What Communities Should Ask For 43
The Public Interest Standard 44
Part Two - Physical and Environmental Impacts 45
5 - Water 47
The Problem With "Low Water" Claims 47
Withdrawal, Consumption, and Discharge 48
The Source Matters 48
Drought and Climate Stress 49
Water Rights, Priority, and Public Control 49
Indigenous Rights and Watershed Governance 50
Water Quality and Discharge 50
Construction Water 50
The Hidden Water in Electricity 51
Core Questions 51
Water Demand 51
Water Source 51
Cooling System 51
Closed-System Claims 52
Discharge and Water Quality 52
Drought and Emergency Conditions 52
Public Cost and Infrastructure 53
Monitoring and Accountability 53
Red Flags 53
What Communities Should Ask For 54
The Public Interest Standard 54

6 - Electricity and Grid Burden 55
The Grid Is Not a Blank Plug 55
Power Demand Must Be Disclosed Clearly 56
Transmission, Substations, and Grid Upgrades 56
Ratepayer Costs and Public Subsidy 56
Grid Reliability and Public Priority 57
Fossil Backup and Hidden Emissions 57
Renewable Claims Must Be Specific 58
Alternative Energy and Lower-Impact Power Options 58
Battery Storage 58
Behind-the-Meter Power and Private Generation 59
Energy Efficiency Is Not the Same as Low Impact 59
Core Questions 59
Power Demand 59
Grid Capacity 60
Cost and Ratepayer Burden 60
Reliability and Curtailment 60
Renewable Energy Claims 61
Alternative Energy Assessment 61
Backup Power 61
Battery Storage 62
Private or Behind-the-Meter Generation 62
Efficiency and Total Load 62
Red Flags 62
What Communities Should Ask For 63
The Public Interest Standard 63
7 - Land Use and Community Fit 65
Community Fit Is Not Static 65
Farmland and Food Systems 66
Wetlands, Forests, Grasslands, and Natural Areas 66
Housing Proximity and Human Health 67
Schools, Hospitals, Care Facilities, and Vulnerable Populations 67
Wildlife Corridors and Habitat Connectivity 67
Transportation Routes and Construction Access 68
Security, Fencing, and Community Character 68
Future Expansion and Development Pressure 68

Compatibility With Municipal and Regional Plans 69
Core Questions 69
Site Selection 69
Current Land Use 69
Future Land Use 69
Farmland 70
Wetlands, Forests, Grasslands, and Natural Areas 70
Housing and Sensitive Uses 70
Wildlife and Habitat 71
Transportation and Access 71
Security and Community Character 71
Future Expansion 71
Red Flags 71
What Communities Should Ask For 72
The Public Interest Standard 72
8 - Sound, Vibration, and Light 75
The Problem With Average Sound 75
All Frequencies Matter 76
Measurement Points Matter 76
Nighttime Sound Is Different 77
Continuous Operation and Cumulative Sound 77
Backup Generators and Testing 78
Construction Noise and Vibration 78
Light Pollution and Night Operations 78
Homes, Health, and Sleep 79
Livestock, Wildlife, and Ecosystems 79
Ongoing Measurement and Real-Time Reporting 79
Core Questions 80
Sound Modelling 80
Frequency Range and Metrics 80
Measurement Points 81
Operations 81
Backup Generators 81

Construction Noise and Vibration 81
Light 81
Homes, Livestock, Wildlife, and Sensitive Sites 82
Ongoing Monitoring and Reporting 82
Red Flags 82
What Communities Should Ask For 83
The Public Interest Standard 83
9 - Heat, Cooling, and Waste Heat 85
Heat Is Not Gone Because It Is Moved 85
Cooling Methods Matter 85
Heat Island Effects 86
Waste Heat: Burden or Public Benefit? 86
District Heating and Community Energy 87
Thermal Pollution and Water Impacts 87
Emergency Cooling and Failure Scenarios 88
Climate Change and Future Conditions 88
Cumulative Thermal Burden 89
Core Questions 89
Heat Production 89
Cooling Method 89
Heat Island Effects 90
Waste Heat Recovery 90
District Energy 90
Thermal Pollution and Discharge 91
Equipment Failure and Emergency Cooling 91
Future Climate and Full Buildout 91
Monitoring and Accountability 91
Red Flags 92
What Communities Should Ask For 92
The Public Interest Standard 93
10 - Air, Emissions, and Backup Systems 95
Backup Power Is Not a Footnote 95
Diesel Generators and Gas Turbines 95
Testing Schedules Matter 96

Emergency Operation and Grid Stress 96
Particulate Emissions and Local Air Quality 97
Greenhouse Gas Emissions 97
Batteries and Fire Risk 97
Fire Suppression Chemicals and Emergency Releases 98
Refrigerants, Coolants, and Chemical Systems 98
Construction Emissions 98
Cumulative Emissions 98
Monitoring and Real-Time Reporting 99
Core Questions 99
Backup Systems 99
Diesel Generators and Gas Turbines 99
Testing Schedules 100
Air Quality 100
Greenhouse Gases 100
Battery Systems 101
Fire Suppression 101
Refrigerants, Coolants, and Chemicals 101
Construction Emissions 101
Cumulative Impacts 102
Monitoring and Reporting 102
Red Flags 102
What Communities Should Ask For 103
The Public Interest Standard 103
11 - Animals, Plants, Agriculture, and Ecosystems 105
Ecosystems Are Not Empty Space 105
Livestock and Farm Animals 106
Crops, Soil, and Agricultural Production 106
Pollinators and Insects 106
Birds, Bats, and Migration 107
Amphibians, Reptiles, and Small Wildlife 107
Aquatic Life and Waterways 107
Wetlands, Forests, Grasslands, and Habitat Networks 108
Fencing, Barriers, and Fragmentation 108
Noise, Vibration, and Light as Ecological Impacts 108

Heat, Microclimates, and Plant Life 109
Chemicals, Spills, and Runoff 109
Cumulative Ecological Disruption 109
Monitoring After Approval 109
Core Questions 110
Existing Ecological Conditions 110
Livestock and Farm Animals 110
Crops, Soil, and Agriculture 110
Pollinators and Insects 111
Birds and Bats 111
Amphibians, Reptiles, and Small Wildlife 111
Aquatic Life 111
Habitat and Connectivity 112
Noise, Light, Heat, and Air 112
Chemicals, Runoff, and Spills 112
Cumulative Impacts 112
Monitoring and Accountability 113
Red Flags 113
What Communities Should Ask For 113
The Public Interest Standard 114
12 - Cumulative Impacts 115
The Problem With Project-by-Project Approval 115
The First Project Is Often the Most Important 116
Full Buildout Must Be Assessed 116
Infrastructure as a Growth Signal 117
Water Cumulative Impacts 117
Electricity Cumulative Impacts 117
Land and Habitat Cumulative Impacts 118
Noise, Light, Heat, and Air Cumulative Impacts 118
Industrial Clustering and Community Identity 118
The Problem of Split Jurisdiction 118
Time Matters 119
Growth Caps and Trigger Points 119
Core Questions 119
Buildout Pattern 119

Infrastructure 120
Water 120
Electricity 120
Land Use 121
Noise, Light, Heat, and Air 121
Transportation 121
Ecosystems 121
Public Finance 122
Governance 122
Monitoring and Accountability 122
Red Flags 122
What Communities Should Ask For 123
The Public Interest Standard 123
Part Three: Data, Power, and Sovereignty 125
13 - Data Sovereignty 125
Data Sovereignty Is More Than Data Location 125
Foreign Laws and Compelled Access 126
Public-Sector Data 126
Health, Education, Courts, Policing, and Social Services 127
Indigenous Data Sovereignty 127
Municipal, Provincial, State, and National Sovereignty 128
Ownership, Control, and Corporate Structure 128
Cloud Architecture and Cross-Border Data Movement 129
Encryption and Key Control 129
Artificial Intelligence and Secondary Use 129
Economic Development and Digital Dependency 130
Security, Breach, and Accountability 130
Core Questions 130
Data Categories 130
Public-Sector Data 131
Ownership and Control 131
Foreign Legal Access 131
Indigenous Data Sovereignty 132

Data Residency and Movement 132
Encryption and Technical Control 132
AI and Secondary Use 133
Critical Infrastructure and Dependency 133
Accountability and Remedies 133
Red Flags 133
What Communities Should Ask For 134
The Public Interest Standard 135
14 - Ownership, Tenants, and Corporate Structure 137
The First Layer Is Not Enough 137
Beneficial Ownership and Control 138
Land, Building, Servers, and Operations 138
Tenants and End Users 139
Subsidies and Who Receives Them 139
Liability and Risk 140
Corporate Restructuring and Sale 140
Financing and Debt 141
Corporate Track Record 141
Local Incorporation and Public Messaging 141
Core Questions 142
Ownership Structure 142
Land, Building, and Equipment 142
Foreign Ownership of Land 142
Operator and Control 143
Tenants and Users 143
Subsidies and Public Benefits 143
Liability 144
Sale, Transfer, and Restructuring 144
Financing and Investors 144
Corporate Track Record 145
Transparency 145
Red Flags 145
What Communities Should Ask For 146

The Public Interest Standard 146
15 - Cybersecurity and Critical Infrastructure 147
Private Infrastructure, Public Dependence 147
Cyberattack and System Failure 147
Critical Public Services 148
Physical Security and Public Impact 148
Redundancy, Backups, and Continuity 149
Supply Chain and Vendor Risk 149
Remote Access and Administrative Control 149
Incident Reporting and Public Notice 150
Public Costs of Cybersecurity and Emergency Preparedness 150
Core Questions 150
Critical Infrastructure Status 150
Cybersecurity Risk 151
Public Service Continuity 151
Physical Security 151
Supply Chain and Vendors 151
Remote Access 152
Incident Reporting 152
Emergency Planning 152
Accountability 153
Red Flags 153
What Communities Should Ask For 153
The Public Interest Standard 154
16 - Privacy, Surveillance, and Public Data 155
Public Data Is Not Ordinary Data 155
Privacy Is Not Just Security 155
Surveillance Infrastructure 156
Facial Recognition and Biometric Data 156
Policing, Immigration, Courts, and Corrections 157
Health, Education, and Children's Data 157
Smart Cities and Sensor Networks 157
Predictive Analytics and Public-Sector AI 158
Data Linking and Function Creep 158
Vendor Power and Democratic Oversight 158
Consent, Notice, and Choice 159
Retention, Deletion, and the Right to Be Forgotten 159
Transparency and Public Registers 159
Core Questions 160

Public Data 160
Personal and Sensitive Data 160
Surveillance Uses 160
Facial Recognition and Biometrics 160
Public-Sector AI and Predictive Analytics 161
Data Linking and Secondary Use 161
Vendor Control 161
Consent, Notice, and Rights 162
Retention and Deletion 162
Transparency and Oversight 162
Harm and Remedies 162
Red Flags 163
What Communities Should Ask For 163
The Public Interest Standard 164
Part Four: Economics and Public Risk 165
17 - Jobs and Economic Claims 165
Construction Jobs Are Not Permanent Jobs 166
Permanent Jobs and Automation 166
Local Hiring 167
Job Quality 167
Public Cost Per Job 167
Tax Revenue Claims 168
Local Business Benefits 168
Opportunity Cost 168
Displacement and Housing Pressure 169
Labour Conditions and Worker Safety 169
Promises Must Be Enforceable 169
Core Questions 170
Job Numbers 170
Local Hiring 170
Job Quality 170
Public Cost Per Job 171
Tax Revenue 171

Local Business and Procurement 171
Opportunity Cost 171
Housing and Community Services 172
Enforcement 172
Red Flags 172
What Communities Should Ask For 173
The Public Interest Standard 173
18 - Tax Incentives and Public Subsidies 175
Subsidies Should Be Named 175
The Full Public Cost 176
Tax Breaks and Forgone Revenue 176
Discounted Electricity and Water 176
Infrastructure Subsidies 177
Grants, Loans, and Financial Support 177
Subsidies Across Multiple Levels of Government 177
Who Receives the Benefit? 178
Clawbacks and Conditions 178
Time Limits and Review Points 179
Public Transparency 179
Public Return on Public Investment 179
Core Questions 179
Subsidy Identification 179
Full Public Cost 180
Tax Incentives 180
Electricity and Water Discounts 180
Infrastructure 181
Recipients and Beneficiaries 181
Public Return 181
Clawbacks and Enforcement 181
Time Limits and Review 182
Transparency 182
Red Flags 182
What Communities Should Ask For 183
The Public Interest Standard 183

19 - Infrastructure Costs and Ratepayer Burden 185
The Public Bill Is Not Always Obvious 185
Direct Costs and Indirect Costs 185
Ratepayer Burden 186
Grid Reinforcement and Electrical Infrastructure 186
Water and Sewer Infrastructure 187
Roads, Bridges, and Transportation Infrastructure 187
Emergency Services and Fire Capacity 187
Public Staff Time and Administrative Capacity 188
Maintenance and Replacement Costs 188
Existing Infrastructure and Deferred Maintenance 189
Oversizing and Future Development 189
Development Charges and Cost Recovery 189
Core Questions 190
Full Infrastructure Cost 190
Electricity and Grid 190
Water and Sewer 190
Roads and Transportation 190
Emergency Services 191
Public Administration 191
Maintenance and Replacement 191
Existing Infrastructure Condition 191
Oversizing and Future Growth 191
Ratepayer and Taxpayer Impact 192
Cost Recovery 192
Red Flags 192
What Communities Should Ask For 193
The Public Interest Standard 193
20 - Decommissioning and Exit Plans 195
Decommissioning Should Be Planned Before Approval 195
Equipment Ages 195
Electronic Waste and Hardware Turnover 196
Tenants May Leave 196
Companies Sell and Restructure 197
Obsolescence and Repurposing 197

Stranded Infrastructure 197
Environmental Cleanup 198
Data Disposal and Digital Exit 198
Bonds, Reserve Funds, and Financial Security 199
Decommissioning Triggers 199
Site Restoration 199
Public Reporting and Oversight 200
Core Questions 200
Lifespan and Obsolescence 200
Tenants and Use Changes 200
Ownership Changes 201
Physical Decommissioning 201
Environmental Cleanup 201
Data Exit 202
Stranded Infrastructure 202
Financial Security 202
Decommissioning Triggers 202
Site Restoration 203
Public Oversight 203
Red Flags 203
What Communities Should Ask For 204
The Public Interest Standard 204
Part Five: Accountability After Approval 207
21 - Monitoring, Reporting, and Enforcement 207
Approval Is Not Accountability 208
Real-Time Data Versus Company Summaries 208
Monitoring Must Measure the Right Things 208
Monitoring Locations Matter 209
Baseline Data 209
Independent Monitoring 209
Public Dashboards and Open Data 210
Complaints Are Data 210
Enforcement Must Have Consequences 210
Reporting During Emergencies 211
Monitoring Future Phases and Expansion 211

Long-Term Accountability 211
Core Questions 212
Water Monitoring 212
Power Monitoring 212
Emissions Monitoring 212
Noise, Vibration, and Light Monitoring 212
Heat and Cooling Monitoring 213
Ecological Monitoring 213
Public Complaints 213
Public Reporting 214
Independence and Auditing 214
Enforcement 214
Expansion and Change 215
Red Flags 215
What Communities Should Ask For 215
The Public Interest Standard 216
22 - Emergency Planning 217
Emergency Planning Before Approval 217
Fire and Explosion 217
Battery Failure and Thermal Runaway 218
Diesel, Fuel, and Generator Emergencies 218
Chemical Releases and Fire Suppression Systems 219
Water Contamination and Runoff 219
Cyberattack and Digital Emergencies 220
Grid Failure and Power Emergencies 220
Extreme Heat, Cooling Failure, and Heat Waves 220
Flood, Stormwater, and Severe Weather 221
Wildfire and Smoke 221
Evacuation and Shelter-in-Place 222
Emergency Service Capacity 222
Emergency Communication and Public Notice 222
Core Questions 223
Emergency Risk Assessment 223
Fire and Explosion 223

Battery Failure 223
Diesel, Fuel, and Generators 224
Chemicals and Fire Suppression 224
Water Contamination and Runoff 224
Cyberattack 224
Grid Failure and Power Emergency 225
Extreme Heat and Cooling Failure 225
Flood, Wildfire, and Severe Weather 225
Evacuation and Shelter-in-Place 225
Emergency Services 226
Communication and Reporting 226
Drills and Review 226
Red Flags 226
What Communities Should Ask For 227
The Public Interest Standard 227
23 - Conditions, Clawbacks, and Public Remedies 229
Conditions Must Be Specific 229
Promises Used to Win Approval Should Become Legal Obligations 230
Clawbacks 230
Escalating Penalties 230
Permit Suspension and Operating Restrictions 231
Future Phases Should Be Conditional 231
Public Trigger Rights 231
Public Remedies 232
Conditions Should Survive Sale or Restructuring 232
Reporting Failures Are Violations 232
Independent Enforcement 233
Enforcement Must Be Public 233
Core Questions 233
Conditions 233
Clawbacks 234
Permits and Operating Limits 234
Escalating Penalties 234

Public Trigger Rights 235
Reporting and Transparency 235
Public Remedies 235
Sale, Transfer, and Restructuring 236
Enforcement Authority 236
Future Phases 236
Red Flags 237
What Communities Should Ask For 237
The Public Interest Standard 238
24 - Community Benefit Agreements 239
Benefits Should Match the Burden 239
Local Hiring and Training 240
Local Procurement and Small Business Access 240
Public Broadband and Digital Access 240
District Heating and Waste Heat Use 241
Water Offsets and Watershed Benefits 241
Environmental Restoration 241
Emergency Service Funding 241
Public Reporting and Transparency 242
Community Governance 242
Indigenous Community Benefits and Rights 242
Enforceability 243
Benefits Should Survive Sale and Expansion 243
Core Questions 243
Agreement Structure 243
Local Hiring and Training 244
Local Procurement 244
Public Broadband and Digital Access 244
District Heating and Waste Heat 244
Water Offsets and Watershed Benefits 245
Environmental Restoration 245
Emergency Services 245
Public Reporting 246
Community Governance 246

Enforcement 246
Red Flags 246
What Communities Should Ask For 247
The Public Interest Standard 248
Addendum A 249
Artificial Intelligence 249
AI Is Not Only a Computing Question 249
The Data Center as AI Infrastructure 250
Training, Inference, and Demand 250
AI and Personal Data 251
Public Data and AI 251
AI, Surveillance, and Public Power 252
AI Bias and Historical Data 252
Copyright, Creative Work, and Cultural Data 253
AI and Indigenous Data Sovereignty 253
AI and Environmental Demand 253
AI Regulation Is Not Enough 254
Data Access as the Immediate Point of Control 254
Core Questions 255
AI Use 255
Data Sources 255
Consent and Control 255
Public-Sector AI 255
Surveillance and Biometrics 256
Bias, Accuracy, and Harm 256
Environmental and Infrastructure Demand 256
Vendor and Secondary Use 256
Transparency and Accountability 257
Red Flags 257
What Communities Should Ask For 257
The Public Interest Standard 258
Addendum B 259
Questions for Public Hearings 259
1. What Is Actually Being Proposed? 259

2. Who Benefits? 260
3. Public Consultation and Consent 260
4. Water 260
5. Electricity and Grid Burden 260
6. Land Use and Community Fit 261
7. Sound, Vibration, and Light 261
8. Heat and Cooling 261
9. Air, Emissions, and Backup Power 262
10. Wildlife, Livestock, Crops, and Ecosystems 262
11. Cumulative Impacts 262
12. Data Sovereignty, Privacy, and Surveillance 263
13. Ownership and Corporate Structure 263
14. Jobs and Economic Claims 263
15. Taxes, Subsidies, and Public Costs 264
16. Infrastructure and Ratepayer Burden 264
17. Emergency Planning 264
18. Monitoring and Public Reporting 264
19. Enforcement and Public Remedies 265
20. Decommissioning and Exit Plans 265
21. Community Benefits 266
Final Public Hearing Questions 266
A Closing Statement for Public Hearings 266

Addendum C 269

Documents to Request 269

1. Project Description and Application Documents 270
2. Ownership and Corporate Structure 270
3. Power, Grid, and Electricity Documents 271
4. Water Documents 271
5. Wastewater, Sewer, and Discharge Documents 272
6. Environmental Assessment Documents 273
7. Sound, Vibration, and Light Documents 273
8. Heat and Cooling Documents 274
9. Air, Emissions, and Backup System Documents 275
10. Traffic, Roads, and Transportation Documents 275
11. Infrastructure Cost and Ratepayer Documents 276
12. Tax, Subsidy, and Incentive Documents 276
13. Jobs and Economic Development Documents 277
14. Emergency Planning Documents 277
15. Cybersecurity, Privacy, Public Data, and AI Documents 278
16. Monitoring, Reporting, and Enforcement Documents 279

17. Conditions, Clawbacks, and Public Remedies Documents 279
18. Community Benefit Agreement Documents 280
19. Decommissioning and Exit Documents 281
20. Indigenous Rights, Consultation, and Governance Documents 281
21. Public Communication Documents 282
If Documents Are Withheld 282
Public Records Request Template 282
The Public Interest Standard 283

Part One: Before the Approval

1 - What Is Actually Being Proposed?

Before a community can evaluate a data center, it has to know what is actually being proposed.

That may sound obvious.

It is not.

A project may be introduced as a technology campus, cloud facility, digital infrastructure project, innovation hub, advanced computing site, AI-ready development, hyperscale investment, enterprise data center, secure storage facility, or economic development opportunity.

Those labels may be useful for marketing.

They are not enough for public review.

The first public-interest question should always be:

What is this?

Not what is it called.

Not how is it being promoted.

Not what does the press release say.

Not what does the artist rendering show.

What is actually being built, who will control it, what will it do, how large can it become, and what future rights are being approved with it?

A community cannot meaningfully evaluate water use, electricity demand, land impact, emergency risk, public cost, surveillance concerns, or economic benefit until the basic identity of the project is clear.

The Problem With Vague Proposals

Many data center proposals begin with broad language.

The public may be told that the facility will support digital services, cloud computing, innovation, artificial intelligence, business growth, secure storage, or regional competitiveness. The language may sound modern and harmless. It may avoid technical detail. It may emphasize jobs, investment, and opportunity.

But vague language can hide major differences.

A small enterprise data center is not the same as a hyperscale campus.

A colocation facility is not the same as a single-tenant AI training facility.

A research computing site is not the same as a crypto-mining operation.

A government records facility is not the same as a private surveillance analytics platform.

A first-phase building is not the same as a long-term data center district.

A project should not be approved on the basis of a general category when the impacts depend on the specific use.

If the public is asked to approve "a data center," the public should ask what kind.

Facility Type

The type of facility matters.

A data center may be designed for cloud storage, enterprise computing, colocation, high-performance computing, artificial intelligence training, AI inference, streaming, financial services, government data, health systems, education platforms, military or defence work, surveillance analytics, smart-city systems, cryptocurrency mining, research computing, or a mix of uses.

Each type may create different demands.

Some facilities require enormous electricity loads but relatively few workers. Some require high-density cooling. Some may need large water systems. Some may involve sensitive public data. Some may create cybersecurity or surveillance concerns. Some may have rapid hardware turnover. Some may operate as neutral landlords for tenants the public never sees.

The public should not accept a project description that says only "data center."

The facility type should be stated plainly.

If the future use is unknown, that uncertainty should not be treated as harmless. Unknown use means unknown impact.

Scale

Scale changes everything.

A data center proposal should disclose its size in terms the public can understand. That includes land area, building footprint, floor area, number of buildings, number of phases, power demand, water demand, backup generation, cooling systems, construction timeline, and full-buildout capacity.

A project may be presented as one building while the site plan reserves land for several more. It may apply for one phase while infrastructure is sized for a much larger campus. It may describe initial power demand while holding rights to expand far beyond that demand later. It may show a modest first stage while seeking zoning, water access, utility service, and road upgrades that make a much larger development possible.

The public should ask whether the proposal is being assessed at its first phase or at full buildout.

The first phase may be the only part shown at the public hearing.
It may not be the project the community is actually being asked to accept.

Purpose

A data center should disclose what it is for.
Will it store data?
Will it process data?
Will it train AI systems?
Will it run AI inference?
Will it support public services?
Will it support private cloud services?
Will it support surveillance tools?
Will it support health, education, policing, immigration, financial, military, or government systems?
Will it support cryptocurrency mining?
Will it support commercial tenants not yet identified?
Purpose matters because public impacts are tied to actual use.

A facility used for government records raises different questions than a facility used for commercial AI training. A facility that hosts school or health data raises different questions than one that hosts entertainment streaming. A facility that supports facial recognition, predictive policing, immigration enforcement, or public-sector AI raises civil rights and privacy questions that ordinary storage may not.

The public should not be told that purpose is irrelevant because the building is only infrastructure.

Infrastructure exists to serve something.
The public has the right to know what.

Owner

The owner matters.

A data center proposal should identify who owns the land, who owns the building, who owns the equipment, who owns the project company, who owns the parent company, and who ultimately benefits from the approval.

The applicant may be a local subsidiary, numbered company, special-purpose vehicle, real estate investment trust, private equity structure, joint venture, foreign-controlled corporation, or newly created entity with limited assets. The public may see one name on the application while control, profit, and liability sit elsewhere.

Ownership affects accountability.

If the project receives tax breaks, infrastructure upgrades, water access, grid capacity, subsidies, or land-use approvals, the public should know who receives the benefit. If something goes wrong, the public should know who is responsible. If the facility is sold, the public should know whether obligations survive.

A community should not approve a project without knowing who stands behind it.

Operator

The owner and operator may not be the same.

One company may own the land. Another may own the building. Another may operate the facility. Another may manage security. Another may own the servers. Another may provide cloud services. Another may lease space to tenants. Another may control the data. Another may receive public subsidies.

The public should ask who will actually run the facility.

Who controls daily operations?

Who manages power use?

Who manages cooling?

Who controls generator testing?

Who responds to emergencies?

Who handles complaints?

Who reports monitoring data?

Who is responsible for compliance?

If the operator is not known, that should be disclosed.

If the operator can change without public review, that should be disclosed too.

A project cannot be accountable if the responsible party is unclear.

Tenants and End Users

Tenants matter.

A data center may operate as a single-tenant facility, a multi-tenant colocation site, a cloud region, or a campus where future users are not yet identified. The public may be told that tenant information is confidential, commercially sensitive, or not finalized.

That may be common in industry.

It is still a public-interest problem.

Tenants determine many of the impacts and risks. They may affect power demand, water use, cooling intensity, hardware turnover, backup needs, data sovereignty, privacy, cybersecurity, surveillance concerns, public-sector involvement, and community benefit.

A facility hosting ordinary business data is not the same as one hosting AI training clusters, biometric surveillance systems, public health records, school platforms, immigration systems, defence contractors, or crypto mining operations.

The public should ask:

Who will use this facility?

If the answer is not known, then approval conditions should define what uses are allowed, what uses are prohibited, and what tenant changes trigger public review.

A blank tenant list should not become a blank cheque.

Timeline

Timeline matters because impacts occur in stages.

A proposal should identify the expected timeline for planning, approval, construction, connection, operation, expansion, and decommissioning. It should also disclose when major infrastructure will be built, when water and power demand begin, when generator testing begins, when tenants arrive, when public benefits begin, and when tax incentives or subsidies take effect.

Construction impacts may occur before the public sees any benefit. Road damage, noise, dust, traffic, worker housing pressure, land clearing, drainage changes, and public staff burden may begin early.

Utility impacts may occur before the facility is fully occupied. Substations, transmission lines, water systems, sewer upgrades, and road changes may be built in anticipation of future demand.

Economic benefits may be delayed, reduced, or dependent on tenant arrival.

The public should ask not only what is promised, but when.

A timeline should show what the community gives up, what the company receives, and when the promised public benefits actually arrive.

Expansion Rights

Expansion rights are one of the most important parts of a proposal.

A data center may seek approval for one building while securing rights that allow multiple future buildings. It may request zoning that permits a broader range of uses. It may build infrastructure sized for expansion. It may acquire adjacent land. It may negotiate water, power, road, or tax arrangements that anticipate future phases. It may present the first phase as modest while designing the site for a much larger campus.

The public should ask what is being approved now.

Is approval limited to the first building?

Does it allow future buildings as of right?

Does it allow expansion without new hearings?

Does it allow increased water use?

Does it allow increased power demand?

Does it allow more generators?

Does it allow different tenants?

Does it allow a shift to AI, crypto mining, surveillance, or other high-impact uses?

Does it allow future phases to proceed administratively?

The first approval may be the moment when the public has the most leverage.

That leverage should not be surrendered unknowingly.

Single Facility or Larger Campus?

A data center should be identified as either a single facility or part of a larger campus.

This distinction matters.

A single facility may have one set of impacts. A campus may create an entirely different scale of water demand, electricity demand, road use, sound, light, heat, emissions, security footprint, emergency planning, tax arrangements, and land-use change.

A campus may also create cumulative impacts that are not visible if each building is reviewed separately.

The public should ask whether the proposed building is the project or simply the first visible piece of a larger plan.

Signs of a larger campus may include large land assembly, oversized infrastructure, multiple pads, phased site plans, planned substations, future road alignments, major water or sewer upgrades, transmission corridors, adjacent parcels, broad zoning permissions, or economic development language about a technology district.

A project should not be assessed as a single building if the real plan is a campus.

Existing Infrastructure Capacity

A data center proposal should not be evaluated on a blank map.

It should be evaluated against the condition of the infrastructure that already exists.

Many communities have aging roads, limited water capacity, sewer constraints, stormwater problems, bridge repair needs, strained fire services, grid limitations, or deferred maintenance. A data center may be proposed into systems that are already under pressure.

The public should ask whether existing infrastructure can actually support the project.

Can the roads handle construction traffic and heavy loads?

Can the water system handle demand without affecting residents, farms, public services, or future housing?

Can the sewer system handle discharge?

Can the stormwater system manage runoff?

Can the grid support the load?

Can fire services respond safely?

Can emergency access be maintained?

If upgrades are needed, the public should know who pays.

If upgrades are oversized for future expansion, the public should know that too.

A project should not be allowed to appear feasible because the cost of making it feasible has been pushed into future budgets.

The Importance of Plain Language

The public should not need to decode industry language to understand what is being proposed.

Terms like hyperscale, colocation, cloud region, AI-ready, high-performance computing, liquid cooling, power usage effectiveness, edge computing, redundancy, renewable-backed, net-zero, digital infrastructure, or advanced computing may be meaningful to specialists. They may also obscure more basic questions.

How big is it?

How much power will it use?

How much water will it use?
Who owns it?
Who operates it?
Who uses it?
What can it become?
Who pays for it?
Who is accountable?

Every proposal should include a plain-language description of the project.

If residents cannot explain what is being proposed after reading the public materials, the materials have failed.

Core Questions

Facility Type

What kind of data center is being proposed?
Is it cloud storage?
Is it colocation?
Is it enterprise computing?
Is it high-performance computing?
Is it AI training?
Is it AI inference?
Is it cryptocurrency mining?
Is it government data storage?
Is it public-sector computing?
Is it surveillance analytics?
Is it a mixed-use facility?
Can the facility change uses later?
What uses are prohibited?

Scale

How many buildings are proposed?
How much land is involved?
What is the building footprint?
What is the total floor area?
What is the first-phase size?
What is the full-buildout size?
What is the maximum power demand?
What is the maximum water demand?

How many generators, batteries, cooling systems, substations, and utility connections are planned?

How large can the facility become without new public approval?

Purpose

What will the facility do?
What services will it support?
Will it store data?
Will it process data?
Will it train AI systems?
Will it run AI services?
Will it support public-sector systems?
Will it support private commercial systems?
Will it support sensitive data?
Will it support policing, immigration, health, education, courts, utilities, defence, or surveillance systems?
Will the purpose be restricted by permit conditions?

Owner

Who owns the land?
Who owns the building?
Who owns the equipment?
Who owns the applicant?
Who owns the parent company?
Who is the beneficial owner?
Is any owner foreign-controlled?
Is any owner a private equity fund, real estate investment trust, special-purpose vehicle, numbered company, subsidiary, or affiliate?
Who receives tax benefits, subsidies, land value increases, or public infrastructure benefits?
Who is liable if promises are not kept?

Operator

Who will operate the facility?
Is the operator the same as the owner?
Can the operator change?
Who is responsible for compliance?
Who handles public complaints?
Who controls generator testing?
Who manages emergency response?
Who reports monitoring data?
Who is accountable if operations violate approval conditions?

Tenants and Users

Who are the tenants?
Are tenants known?

Will tenants be publicly disclosed?
What types of tenants are allowed?
What types of tenants are prohibited?
Can tenants change without public notice?
Can the facility shift to AI training, crypto mining, surveillance, defence, policing, immigration, or other high-impact uses?
Will tenant changes trigger public review?
Will tenant uses affect water, power, heat, emissions, privacy, cybersecurity, or public services?

Timeline

When will construction begin?
How long will construction last?
When will the facility connect to the grid?
When will water use begin?
When will generator testing begin?
When will operations begin?
When will tenants arrive?
When will public benefits begin?
When do tax incentives begin?
When are future phases expected?
When will the facility be reviewed after opening?
What is the planned lifespan of the project?

Expansion Rights

Is this approval for one building or multiple phases?
Can future phases proceed without new public hearings?
Can power demand increase without new review?
Can water demand increase without new review?
Can additional generators be added without new review?
Can the facility expand onto adjacent land?
Is infrastructure being built for future expansion?
Can zoning allow larger development than what is currently shown?
What conditions apply before expansion?

Campus or Single Facility

Is this a single data center?
Is it the first phase of a larger campus?
Is it part of a planned technology district?
Are nearby parcels owned, optioned, or controlled by the same developer or affiliates?
Are roads, substations, water pipes, sewer systems, or transmission lines being sized for more than the first building?
Are other data centers planned nearby?

Has full-campus impact been assessed?

Existing Infrastructure

Can existing roads handle the project?
Can existing water systems handle it?
Can existing sewer systems handle it?
Can existing stormwater systems handle it?
Can existing grid infrastructure handle it?
Can existing emergency services handle it?
What upgrades are required?
Who pays for upgrades?
Are upgrades sized for this project or future growth?
Will public infrastructure capacity be diverted from housing, farms, public services, or local businesses?

Public Understanding

Is there a plain-language project description?
Are technical terms explained?
Are maps, phasing plans, ownership charts, utility demands, and infrastructure requirements public?
Can residents understand what is being proposed without relying on company assurances?
Can decision-makers clearly describe what they are approving?

Red Flags

A proposal deserves greater scrutiny when the public hears:
"This is just digital infrastructure."
"The exact tenants are not known yet."
"Future phases will be addressed later."
"The facility is AI-ready."
"The project will be built as market demand requires."
"Power demand depends on tenant needs."
"Water use depends on final design."
"Ownership details are commercially sensitive."
"Tenant information is confidential."
"The first phase is all that is being considered."
"Infrastructure will support future growth."
"Use changes will remain within existing zoning."

A vague project cannot receive meaningful consent.
A first phase cannot be understood without the full buildout.
A tenant list that does not exist cannot be treated as low risk.
A future expansion right is still part of today's decision.

What Communities Should Ask For

Before approval, communities should ask for:

A plain-language project description.

A facility-type disclosure.

A full site plan.

A phasing plan.

A full-buildout plan.

A purpose and use statement.

A list of permitted and prohibited uses.

A land ownership disclosure.

A beneficial ownership disclosure.

An operator disclosure.

A tenant disclosure or tenant-use framework.

A corporate structure chart.

A timeline for construction, operation, expansion, and review.

A full infrastructure capacity assessment.

A statement identifying whether this is a single facility or part of a larger campus.

A disclosure of all expansion rights being requested.

A list of all approvals required.

A table showing which impacts are assessed for first phase only and which are assessed for full buildout.

Clear conditions requiring new public review for major changes in scale, use, ownership, tenants, water demand, power demand, emissions, surveillance use, AI workloads, or expansion.

The Public Interest Standard

No community should be asked to approve a data center it cannot clearly describe.

Before debating benefits, risks, subsidies, jobs, water, power, privacy, or environmental impact, the public must know what is actually being proposed.

What type of facility is it?

How large can it become?

What will it do?

Who owns it?

Who operates it?

Who will use it?

When will it expand?

What rights are being granted today?

And is this truly a single data center, or the first phase of something much larger?

If those questions cannot be answered clearly before approval, the project is not ready for approval.

2 - Who Benefits?

Every data center proposal arrives with a promise of benefit.

- Jobs.
- Investment.
- Tax revenue.
- Innovation.
- Modernization.
- Digital infrastructure.
- Economic growth.
- Regional competitiveness.
- Public-private partnership.
- A place in the future.

Those words may sound public.

But the benefits may not be evenly shared.

A data center can create enormous private value while leaving the public with infrastructure costs, water stress, grid pressure, emergency burdens, tax exemptions, land-use changes, environmental impacts, and long-term obligations. The project may be described as a community opportunity, but the largest gains may flow to landowners, developers, tenants, shareholders, parent companies, utilities, real estate investors, or foreign-controlled entities.

The public should not ask only:

What benefits are being promised?

The better question is:

Who receives the benefit, who carries the burden, and what is legally guaranteed to remain in the community?

A project should not be approved simply because someone benefits.

The public-interest question is whether the community benefits enough, fairly, transparently, and enforceably.

Public Benefit Versus Private Gain

Private gain is not automatically bad.

Companies build projects to make money. Investors expect returns. Developers increase land value. Operators sell services. Tenants gain computing capacity. Utilities may gain large customers. Governments may seek economic development.

But private gain should not be confused with public benefit.

A project can be profitable without being good for the community. It can create investment without creating many permanent jobs. It can increase land value while reducing public control over land. It can generate tax revenue while also receiving tax breaks. It can build infrastructure that appears public but primarily serves one private user. It can bring digital capacity to a region while local residents still lack affordable broadband.

The public should ask what portion of the benefit is private, what portion is public, and what portion is merely assumed.

A benefit should be measured by what the community actually receives, not by the size of the company's announcement.

Who Receives the Money?

The financial benefit of a data center may pass through many hands.

The landowner may profit from a sale or lease. The developer may profit from site preparation, construction, or resale. The building owner may collect rent. The operator may collect service fees. The tenant may gain computing capacity. The parent company may gain market advantage. Investors may gain asset value. Utilities may gain revenue from a large customer. Contractors may gain temporary work. Governments may claim economic development success.

The community may receive some of those benefits.

Or it may mostly receive the impacts.

The public should ask for a clear map of financial benefit.

Who makes money from land conversion?

Who makes money from construction?

Who makes money from utility service?

Who makes money from tax incentives?

Who makes money from public infrastructure upgrades?

Who makes money if the project is sold?

Who receives the long-term profit after construction ends?

If the public is being asked to provide land-use approval, water access, grid capacity, infrastructure support, tax incentives, or political support, it has the right to know who benefits financially.

Land Value and Speculation

A data center proposal can transform land value.

Land that was agricultural, rural, industrial, vacant, or relatively inexpensive may become far more valuable once it is rezoned, serviced, connected to power, granted water access, or included in an economic development plan.

That increase in value may be created partly by public decisions.

A rezoning decision may create private value.

A road upgrade may create private value.

A new substation may create private value.

A water agreement may create private value.

A tax incentive may create private value.

A public announcement may create private value.

The public should ask who captures that value.

If land value rises because public systems support the project, does the public receive a return? Or does the increase flow mainly to private landowners, developers, investors, or future buyers?

A community should not give away public leverage without understanding how much private value it is creating.

Jobs as Benefit

Jobs are one of the most common promises used to justify data center development.

Jobs matter.

But job claims should be specific.

How many jobs are temporary construction jobs?

How many are permanent operational jobs?

How many are local?

How many are full-time?

How many are contracted?

How many require specialized skills not available locally?

How many will still exist five years after opening?

What will they pay?

Will they include benefits?

Will they include training?

Will they be union or non-union?

Will they be accessible to local workers, Indigenous workers, young workers, displaced workers, or underemployed residents?

A project that creates hundreds of construction jobs but only a small number of permanent local jobs should not be described as a long-term employment solution without qualification.

The public should ask whether jobs are real, local, durable, accessible, and enforceable.

Tax Revenue as Benefit

Tax revenue may be a real public benefit.

But only if the project actually pays taxes at a level that exceeds public costs.

A data center may be promoted as a future tax base while also receiving tax abatements, exemptions, rebates, special assessments, payment-in-lieu arrangements, equipment exemptions, or long-term incentive deals. It may require public infrastructure and emergency services while paying reduced taxes. It may increase municipal revenue on paper but shift costs to utility ratepayers, water users, or other levels of government.

The public should ask for net tax benefit, not gross tax benefit.

What will the project pay without incentives?

What will it actually pay?

What public services will it require?

What infrastructure will it trigger?

What costs will be shifted to taxpayers or ratepayers?

How long before the public breaks even?

What happens if revenue projections are wrong?

A tax benefit is not proven by a projection.

It is proven by revenue that remains after public costs are counted.

Infrastructure as Benefit

Developers and governments may argue that infrastructure built for a data center will also benefit the broader community.

Sometimes that may be true.

A road upgrade may improve local access. A water line may serve future development. A grid upgrade may increase regional capacity. Fiber installation may support public broadband. Emergency equipment may help the whole municipality.

But infrastructure should not be called a public benefit simply because it exists.

The public should ask who the infrastructure primarily serves.

Was the road widened for residents, or for construction traffic?

Was the water line sized for housing, or for cooling demand?

Was the substation built for public resilience, or for one private load?

Was emergency capacity expanded for the community, or because the facility creates specialized risk?

Will residents actually be able to use the fiber network?

Will ratepayers pay for infrastructure that mainly benefits the data center?

Infrastructure is a public benefit only if it serves public needs, remains publicly useful, and does not shift private costs onto the community.

Digital Access as Benefit

A data center may be described as digital infrastructure, but that does not mean the surrounding community receives digital access.

A region can host massive computing facilities while residents still lack affordable high-speed internet. Schools, libraries, small businesses, farms, rural households, and low-income residents may remain underserved even as fiber lines, network capacity, and digital infrastructure pass nearby.

The public should ask whether the project improves local digital access.

Will public broadband be expanded?

Will schools and libraries benefit?

Will rural residents benefit?

Will farms and local businesses benefit?

Will affordable internet programs be included?

Will any network infrastructure be available for public use?

Or will the community simply host private digital capacity it cannot access?

A community should not be asked to sacrifice land, water, electricity, or tax capacity for digital infrastructure that bypasses it.

Community Benefit Versus Community Branding

Some benefits are real.

Others are branding.

A donation to a local event, a scholarship fund, a sponsorship, a volunteer day, a public relations campaign, or a community open house may be positive. But those gestures should not be confused with enforceable community return.

A project that receives tax breaks, discounted utilities, water access, grid capacity, public infrastructure, or land-use approval should not satisfy public benefit obligations through symbolic contributions.

The public should ask whether benefits are binding.

Is there a Community Benefit Agreement?

Are local hiring targets enforceable?

Are training commitments funded?

Are public broadband improvements required?

Are water offsets measurable?

Are emergency service contributions guaranteed?

Are environmental restoration commitments legally binding?

Are benefits monitored and reported?

Are clawbacks available if benefits are not delivered?

A benefit that can disappear when budgets tighten is not a public safeguard.

Who Carries the Burden?

Every benefit claim should be paired with a burden question.

Who lives near the facility?

Who hears the noise?

Who sees the light?

Who loses the farmland?

Who shares the watershed?

Who pays higher rates?

Who responds to emergencies?

Who absorbs construction traffic?

Who experiences heat, emissions, or ecological change?

Who loses future land-use options?

Who faces privacy or surveillance risks?

Who carries the consequences if the company sells, downsizes, automates, or leaves?

The people who carry the burden may not be the same people who receive the benefit.

A municipality may receive tax revenue while nearby residents experience noise. A province may claim economic growth while local ratepayers pay infrastructure costs. A company may profit while emergency services absorb new risks. A data center may serve distant customers while local farms compete for water or grid capacity.

Benefit must be evaluated alongside burden.

A project is not fair merely because it benefits someone.

Distribution of Benefits

Public benefit should be examined by distribution.

Do the benefits reach residents?

Do they reach workers?

Do they reach Indigenous governments and communities?

Do they reach farmers?

Do they reach local businesses?

Do they reach schools, hospitals, libraries, and public services?

Do they reach low-income households?

Do they reach people living closest to the project?

Do they reach the people most affected by construction, noise, light, traffic, water use, or environmental change?

A project that creates regional economic statistics but leaves the immediate community with the burdens has not delivered equitable benefit.

The public should ask not only whether benefits exist, but where they land.

Time Matters

Benefits and burdens may arrive on different timelines.

Construction impacts may begin immediately. Land may be cleared immediately. Roads may be disrupted immediately. Public staff time may be consumed immediately. Infrastructure costs may begin before the facility opens. Tax incentives may begin early. Water and power capacity may be reserved before jobs arrive.

Promised benefits may arrive later.

Permanent jobs may depend on future tenants. Tax revenue may depend on incentive periods ending. Community benefits may depend on later agreements. Waste heat recovery may be described as future potential. Public broadband may be delayed. Environmental restoration may take years. Some benefits may never materialize.

The public should ask when each benefit begins and when each burden begins.

A community should not carry immediate costs in exchange for distant, uncertain, or unenforceable benefits.

Core Questions

Financial Benefit

Who profits from the project?

Who owns the land?

Who profits from land sale or lease?

Who profits from construction?

Who profits from operation?

Who profits from utility service?

Who profits from public infrastructure upgrades?
Who profits if the project is sold?
Who receives tax incentives, subsidies, grants, discounted utilities, or public supports?
Who receives the long-term financial return?

Public Benefit

What benefits will remain in the community?
How many permanent local jobs are guaranteed?
What tax revenue is guaranteed?
What local procurement is guaranteed?
What training is guaranteed?
What infrastructure will be publicly useful?
What public broadband improvements are guaranteed?
What emergency service funding is guaranteed?
What environmental restoration is guaranteed?
What water, energy, or community benefits are legally binding?

Jobs

How many construction jobs will be created?
How many permanent jobs will remain after construction?
How many jobs will be local?
How many will be full-time?
How many will be contracted?
What wages and benefits will be paid?
What training will be provided?
Will local workers be able to qualify for the jobs?
Will Indigenous hiring be included where appropriate?
Are job promises enforceable?

Tax Revenue

What taxes would the project pay without incentives?
What taxes will it actually pay?
How long do tax incentives last?
What public services will the facility require?
What infrastructure costs must be counted against tax revenue?
What is the net tax benefit?
How long until the public breaks even?
What happens if tax projections are wrong?
Can tax benefits be revoked if promises are not kept?

Infrastructure Benefit

What infrastructure will be built?
Who will own it?

Who will maintain it?
Who will pay for it?
Who will use it?
Does it primarily serve the project or the public?
Will it support housing, farms, public services, local businesses, broadband, or community resilience?
Will residents pay through taxes or utility rates?
Will the infrastructure create pressure for further development the community has not approved?

Digital Access

Will the project improve public broadband?
Will local residents benefit from new fiber or network infrastructure?
Will schools, libraries, farms, small businesses, and public agencies gain access?
Will low-income households benefit?
Will digital access improvements be legally required?
Will the community host digital infrastructure without being able to use it?

Community Benefits

Will there be a Community Benefit Agreement?
Who negotiates it?
Who enforces it?
What benefits are included?
Are benefits specific, measurable, funded, and time-bound?
Do benefits survive sale or ownership change?
Can benefits be clawed back if not delivered?
Are reports public?
Can the public trigger review?

Burdens

Who lives closest to the facility?
Who will experience construction traffic?
Who will experience noise, vibration, light, or heat?
Who shares the water source?
Who shares the grid?
Who pays through rates or taxes?
Who responds during emergencies?
Who loses land-use options?
Who faces ecological, agricultural, privacy, or public-data risks?
Are burdens and benefits falling on the same people?

Timing

When do construction impacts begin?
When do infrastructure costs begin?
When do water and power commitments begin?
When do tax incentives begin?
When do permanent jobs begin?
When does tax revenue begin?
When do community benefits begin?
When does public reporting begin?
Are benefits delayed while burdens begin immediately?

Red Flags

A benefit claim deserves greater scrutiny when the public hears:
"This project will bring investment."
"The economic impact will be significant."
"This will put the community on the map."
"The project will create jobs."
"Tax revenue will grow over time."
"Infrastructure upgrades will benefit everyone."
"The company is committed to being a good neighbour."
"Community benefits will be discussed later."
"Local hiring will be encouraged."
"Public benefits are difficult to quantify."

Investment is not the same as public benefit.
Jobs are not the same as permanent local employment.
Infrastructure is not a community benefit if the community pays for it.
Goodwill is not an enforceable return.
Economic development is not proven until the benefits remain after the costs are counted.

What Communities Should Ask For

Before approval, communities should ask for:
A full public benefit statement.
A financial beneficiary disclosure.
A land value and public value assessment.
A job creation and job quality assessment.
A local hiring and training plan.
A tax revenue and public cost analysis.
A net public benefit calculation.
A local procurement plan.
A public infrastructure benefit analysis.

A public broadband and digital access plan where applicable.

A Community Benefit Agreement.

A burden distribution assessment.

A timeline showing when benefits and burdens begin.

Independent verification of economic claims.

Legally binding commitments.

Clawbacks, penalties, and public remedies if benefits are not delivered.

The Public Interest Standard

No data center should be approved on the basis of vague benefit claims.

Before approval, the public should know who profits, who pays, who is affected, what benefits are legally guaranteed, when those benefits arrive, and whether the people carrying the burden will share fairly in the return.

A project may create private value.

That is not enough.

If a community is being asked to provide land-use permission, public infrastructure, water access, grid capacity, tax incentives, emergency services, environmental tolerance, or public trust, then the benefit to that community must be real, measurable, local, durable, and enforceable.

The question is not whether someone benefits.

The question is whether the public does.

3 - Who Decides?

A data center is rarely approved by one decision-maker.

One body may approve zoning.
Another may approve water use.
Another may approve road access.
Another may approve transmission lines.
Another may approve power connection.
Another may regulate emissions.
Another may negotiate tax incentives.
Another may hold emergency planning authority.
Another may have jurisdiction over privacy, public data, cybersecurity, or Indigenous rights.

This can make accountability difficult.

A municipality may say water licensing belongs to another authority. A utility may say land use belongs to the municipality. A regulator may say public subsidies are outside its scope. A province or state may say local planning is local. A federal agency may say the project does not trigger federal review. A company may move through each process separately, answering only the questions required in that narrow forum.

The public should not ask only:

Who has legal authority to approve this piece?

The better question is:

Who is responsible for understanding the whole project?

A data center may be divided across permits, licences, approvals, utility agreements, tax arrangements, public consultations, environmental reviews, and infrastructure decisions. But the community experiences the project as one facility, one campus, one load on the grid, one demand on water, one land-use decision, one emergency risk, one set of public costs, and one long-term change to place.

Fragmented approval should not become fragmented accountability.

The Approval Map

Before a community can participate meaningfully, it needs an approval map.

That map should identify every decision required before the project can proceed. It should show which authorities are involved, what each authority controls, what each authority does not control, when decisions will be made, what documents will be considered, whether public input is allowed, and whether decisions can be appealed.

The approval map should include local, regional, provincial, state, federal, utility, water, environmental, emergency, tax, land-use, Indigenous, and regulatory processes where relevant.

Without an approval map, the public may miss the most important decision points.

A zoning hearing may occur before water use is known. A power agreement may be negotiated before public consultation. A tax incentive may be approved before environmental review. A road upgrade may be funded before the facility is fully described. A utility connection may be treated as technical even though it enables the entire project.

The public should not have to discover the process piece by piece.

The process itself should be disclosed.

Municipal and Local Authority

Municipalities often control land use.

They may approve zoning, rezoning, development permits, site plans, road access, local servicing, stormwater, building permits, setbacks, lighting, landscaping, noise bylaws, business licences, local tax arrangements, and public consultation processes.

But municipal authority may be limited.

A municipality may not control the regional grid. It may not issue water licences. It may not regulate federal data systems. It may not control foreign ownership. It may not regulate all air emissions. It may not have authority over transmission lines, highways, privacy law, or Indigenous rights. It may not have staff or technical capacity to evaluate complex data center impacts.

This does not mean municipalities are powerless.

Municipalities can ask questions before approving land use. They can require public disclosure. They can condition approvals where authority allows. They can require development agreements. They can demand cost recovery. They can request independent studies. They can refuse to approve incomplete proposals. They can coordinate with other authorities. They can insist that major off-site impacts be understood before local approval is granted.

A local council should not approve the land-use doorway to a project while claiming the rest of the house is someone else's problem.

Provincial or State Authority

Provincial and state governments may control many of the systems that make data centers possible.

They may oversee electricity policy, water licensing, environmental regulation, utility regulation, transmission planning, economic development incentives, tax credits, highways, labour standards, public health, emergency management, resource use, privacy laws, public-sector procurement, and Indigenous consultation obligations.

They may also actively promote data center development.

This creates a potential conflict.

The same level of government may be trying to attract investment while also being responsible for protecting water, land, ratepayers, public budgets, workers, privacy, and public safety.

The public should ask which provincial or state departments are involved and whether their roles are promotional, regulatory, financial, or oversight-based.

A government should not be allowed to celebrate a project with one hand and quietly weaken public safeguards with the other.

Federal Authority

Federal authority may become relevant when a project affects national infrastructure, cross-border data, Indigenous rights, fisheries, navigable waters, federal lands, national security, foreign ownership, critical infrastructure, air emissions, cybersecurity, public-sector data, defence, immigration systems, federal procurement, or environmental matters within federal jurisdiction.

A federal review may or may not be required.

But the absence of federal review does not mean the absence of federal interest. A data center may support systems used by federal agencies, foreign companies, defence contractors, public cloud providers, or cross-border data flows. It may rely on infrastructure or subsidies connected to national policy. It may raise sovereignty, security, or privacy questions that exceed local planning.

The public should ask whether any federal authority has reviewed the project, declined to review it, funded it, supported it, contracted with it, or assessed its national implications.

If federal agencies benefit from the facility or use its services, that should be disclosed where possible.

Utility Regulators and Grid Authorities

Electricity decisions may be made through utilities, grid operators, transmission planners, energy regulators, public utility commissions, or other technical bodies.

These decisions may seem separate from land-use approval, but they can determine whether the project is possible.

A data center cannot operate without power. If it requires substations, transmission lines, distribution upgrades, transformers, grid reinforcement, new generation, special tariffs, ratepayer cost recovery, demand-response agreements, or curtailment rules, those decisions shape the public impact.

The public should ask who approves the electrical connection and who assesses the effect on ratepayers.

Will the utility disclose project load?

Will grid studies be public?

Will ratepayer impacts be assessed?

Will other users pay for upgrades?

Will the facility receive special treatment during grid emergencies?

Will the public know if power demand increases?

A grid approval should not be treated as a private technical matter when public ratepayers, public reliability, and public infrastructure are involved.

Water Licensing Bodies

Water decisions may be made by municipal utilities, watershed authorities, provincial or state agencies, irrigation districts, groundwater regulators, environmental departments, or other licensing bodies.

These decisions may determine how much water the facility can withdraw, consume, discharge, reuse, or reserve.

The public should ask who controls water access.

Is the source municipal water, groundwater, surface water, reclaimed water, industrial water, stormwater, or another supply?
Who grants permission?
Who monitors use?
Who decides during drought?
Who protects downstream users?
Who evaluates cumulative impacts?
Who enforces limits?
Who can reduce water use if conditions change?

Water approval should not be considered separately from land use, power demand, cooling systems, agriculture, ecosystems, Indigenous rights, or future community growth.

A water licence is not just a technical document.

It is a decision about a shared resource.

Environmental Authorities

Environmental review may be handled by local, regional, provincial, state, or federal bodies, depending on the jurisdiction and the impacts involved.

Some projects may require formal environmental assessment. Others may require narrower studies. Some may avoid full assessment because they fall below thresholds, are split into phases, are classified as ordinary industrial development, or do not trigger specific legal categories.

The public should ask what level of environmental review is required and what level is being avoided.

Does the review include water, power, land, habitat, emissions, noise, light, heat, wildlife, livestock, agriculture, climate, cumulative impacts, and full buildout?
Does it consider future phases?
Does it consider related infrastructure?
Does it consider transmission lines, roads, substations, water systems, and backup power?
Does it consider the impacts of clustered development?

A project should not avoid meaningful review by dividing itself into pieces.

Indigenous Governments and Rights-Holders

Indigenous governments are not stakeholders in the ordinary sense.

They are rights-holders.

Data center development may affect lands, waters, treaty rights, harvesting, cultural sites, wildlife, fish, plants, sacred places, traditional territories, data sovereignty, environmental governance, and future land-use decisions.

Where Indigenous rights, title, treaty obligations, lands, waters, resources, or governance are involved, Indigenous governments must be engaged according to their own laws, protocols, and decision-making processes, not merely invited to comment after plans are advanced.

The public should ask which Indigenous governments may be affected, when they were contacted, what information they received, whether they had enough time and resources to review the project, whether their concerns changed the project, and whether accommodation or consent is required.

Consultation should not be treated as a checkbox.

It should occur early enough to influence whether the project proceeds, where it is located, how it is designed, what conditions apply, and whether it is acceptable at all.

Zoning Boards, Planning Commissions, and Appeals

Many data center decisions move through planning commissions, zoning boards, subdivision authorities, development appeal boards, land-use tribunals, or similar bodies.

These bodies may focus on whether the project fits existing land-use rules.

But data centers may test the limits of existing categories. A zoning code may treat a data center as industrial, warehouse, office, utility, technology, or commercial use even though its actual impacts may differ from all of those categories.

The public should ask whether current zoning rules were designed with data centers in mind.

Do they address power demand?

Water demand?

Backup generators?

Cooling systems?

Noise?

Light?

Security fencing?

Heat?

Emergency planning?

Cybersecurity?

Public data?

Full-buildout impacts?

If existing zoning rules are outdated, the approval process should not pretend they are sufficient.

A new kind of infrastructure may require new public rules.

Public Consultation Rules

Public consultation rules vary widely.

Some processes require formal hearings. Some require mailed notices. Some require open houses. Some require public comment periods. Some require only notice to nearby landowners. Some require no meaningful consultation at all if the use is already permitted. Some allow technical agreements to be finalized without public review.

The public should ask what consultation rules apply and whether they are adequate for a project of this scale.

Was notice sent only to nearby properties, or to the broader community affected by water, power, traffic, taxes, emergency services, and infrastructure?

Were Indigenous governments engaged separately and appropriately?

Were farmers, schools, hospitals, care facilities, local businesses, and vulnerable residents notified?

Were documents available before the meeting?

Were they understandable?

Was enough time provided?

Were meetings held at accessible times and places?

Were online options available?

Were translation, accessibility, or plain-language supports provided?

Will public comments influence the decision?

Consultation is not meaningful if the public learns about the project after the real decisions have already been made.

Public Agencies as Customers

Sometimes public agencies are not only regulators.

They may also be customers.

A government may approve a data center while also planning to use it for public cloud services, health systems, education platforms, policing databases, court records, public-sector AI, smart-city systems, or other public data. A government may promote the project because it aligns with digital modernization or economic development goals.

This creates another accountability question.

If a public agency may benefit from the project, use the project, fund the project, or depend on the project, the public should know.

The role of government should be clear.

Is it regulator?

Customer?

Subsidizer?

Landowner?

Promoter?

Utility owner?

Emergency responder?

Data user?

All of the above?

The more roles a public authority plays, the more transparency is needed.

The Problem of "Not Our Jurisdiction"

One of the most common barriers to public accountability is jurisdictional deflection.

Residents may ask about water at a zoning hearing and be told water is handled elsewhere. They may ask about grid impacts and be told utilities will address them. They may ask about tax incentives and be told that is a separate agreement. They may ask about public data and be told that is a tenant

issue. They may ask about Indigenous rights and be told consultation is another government's responsibility. They may ask about emergency capacity and be told that will be handled later.

Each answer may be technically correct.

Together, they can make meaningful public review impossible.

The public should ask decision-makers to identify every issue outside their jurisdiction and explain which authority is responsible for it, when that authority will decide, how the public can participate, and whether local approval will wait until those answers are known.

A public body should not approve its piece of the project while leaving the public with no forum for the whole.

Core Questions

Approval Process

What approvals are required before the project can proceed?

Which approvals have already been granted?

Which approvals are pending?

Which approvals will occur after zoning or land-use approval?

What is the sequence of decisions?

Which decision is the point of no return?

Can the public see an approval map?

Can approval be paused until all major impacts are known?

Municipal and Local Authority

What decisions will the municipality make?

Does the municipality control zoning, development permits, site plans, local roads, stormwater, noise bylaws, lighting, tax agreements, or local servicing?

What issues are outside municipal authority?

Can the municipality require studies before approval?

Can the municipality impose conditions?

Can the municipality recover infrastructure costs?

Can the municipality refuse approval if information is incomplete?

Can the municipality require future phases to return for public review?

Provincial or State Authority

What provincial or state agencies are involved?

Who controls water licensing?

Who controls electricity policy?

Who regulates utilities?

Who regulates environmental impacts?

Who approves highways or major roads?

Who provides economic development incentives?

Who oversees emergency management?

Who regulates labour, privacy, public health, or public-sector procurement?

Is the province or state promoting the project while also regulating it?

Federal Authority

Are any federal approvals required?

Has any federal review been requested?

Has any federal review been declined?

Are fisheries, navigable waters, federal lands, Indigenous rights, national security, foreign ownership, public data, defence, immigration, or critical infrastructure issues involved?

Will federal agencies use the facility?

Will federal funding, tax credits, procurement, or policy support be involved?

Utility and Grid Decisions

Who approves the electrical connection?

Who approves substations, transmission lines, distribution upgrades, transformers, or grid reinforcement?

Will grid studies be public?

Who assesses ratepayer impacts?

Who decides whether costs are paid by the developer or all users?

Will the public have a chance to participate in utility proceedings?

Will grid approval occur before or after land-use approval?

Water Decisions

Who controls water access?

Who issues water licences or permits?

Who approves municipal water service?

Who approves groundwater use?

Who approves surface water withdrawals?

Who approves discharge?

Who assesses drought risk?

Who protects downstream users?

Who monitors water use?

Who can reduce or suspend water use if conditions change?

Environmental Review

What environmental review is required?

What environmental review is voluntary?

Does the review include full buildout?

Does it include cumulative impacts?

Does it include related infrastructure?

Does it include water, power, land, emissions, noise, heat, light, wildlife, livestock, crops, and climate risk?

Who decides whether the environmental review is sufficient?

Can the public challenge the adequacy of the review?

Indigenous Governments

Which Indigenous governments may be affected?
Were they engaged before key decisions were made?
Were they given full information?
Were they given adequate time and resources?
Were their laws, protocols, and decision-making processes followed?
Were impacts on treaty rights, lands, waters, harvesting, culture, data, and governance assessed?
What accommodation measures are proposed?
Is consent required?
Who decides whether consultation was adequate?

Zoning and Planning

What zoning currently applies?
What zoning change is being requested?
Does current zoning explicitly contemplate data centers?
Does zoning address water, power, backup generation, cooling, sound, heat, light, security, emergency planning, and future expansion?
Can the facility change uses under the proposed zoning?
Can future phases proceed without new hearings?
Can neighbouring land be added later?
Can conditions be attached to zoning or development approval?

Public Consultation

Who was notified?
How were they notified?
How far from the project did notice extend?
Were people affected by water, power, traffic, taxes, emergency services, and infrastructure notified, even if they do not live next door?
Were documents available early enough?
Were technical documents released?
Were plain-language summaries provided?
Were meetings accessible?
Were online options available?
Were translation and disability access provided where needed?
Will public comments affect the decision?

Government Roles

Is any public authority also a customer, funder, promoter, landowner, utility owner, or data user?
Will public agencies use the facility?
Will public data be stored or processed there?
Will public money support the project?
Will government staff promote the project while also reviewing it?

How will conflicts of interest be disclosed and managed?

Accountability

Who is responsible for the whole project?
Who ensures that separate approvals fit together?
Who tracks cumulative impacts?
Who ensures public questions are not lost between jurisdictions?
Who enforces conditions after approval?
Who can reopen approval if new information emerges?
Who can stop the project if major risks are unresolved?

Red Flags

A decision-making process deserves greater scrutiny when the public hears:
"That is outside the scope of this hearing."
"That will be handled by another authority."
"Those details will be finalized later."
"Utility matters are separate."
"Water licensing is a separate process."
"Environmental review is not required."
"Consultation requirements have been met."
"The project complies with existing zoning."
"Future phases will follow normal procedures."
"The public can raise those concerns at another stage."

If an issue is outside one authority's scope, the public should be told whose scope it is in.

If details will be finalized later, the public should be told whether approval can wait.

If consultation requirements have been met, the public should ask whether consultation was meaningful, not merely legal.

A fragmented approval process should not become a maze that prevents public understanding.

What Communities Should Ask For

Before approval, communities should ask for:
A complete approval map.
A list of all authorities involved.
A list of all approvals required.
A timeline showing when each decision will be made.
A description of public participation rights at each stage.
A list of decisions already made.
A list of decisions still pending.
A plain-language explanation of which body controls which issue.

Disclosure of any public agencies that are also customers, funders, promoters, landowners, utility owners, or data users.

A jurisdictional responsibility table covering land use, water, power, grid upgrades, roads, tax incentives, subsidies, environmental review, emergency planning, Indigenous consultation, privacy, public data, cybersecurity, monitoring, and enforcement.

A commitment that major land-use approval will not occur before core water, power, infrastructure, emergency, environmental, Indigenous rights, and public cost questions are answered.

A process for coordinating decisions across jurisdictions.

A public record of all studies, agreements, permits, licences, approvals, and conditions.

A clear statement identifying who is responsible for the whole project.

The Public Interest Standard

No data center should be approved through a process so fragmented that the public cannot tell who is responsible for what.

Before approval, the public should know which authorities decide land use, water access, grid connection, public subsidies, tax incentives, environmental review, emergency planning, Indigenous consultation, public data, privacy, infrastructure costs, monitoring, and enforcement.

A community should not be told that every major concern belongs somewhere else.

If a project requires many approvals, then the public needs one clear map of the approval system.

Who decides matters.

Because when no one is responsible for the whole project, the public is often left responsible for the consequences.

4 - Public Consent and Consultation

Public consultation is often treated as a step in the approval process.

It should be treated as a test of legitimacy.

A data center may affect land, water, electricity, roads, taxes, emergency services, public infrastructure, sound, heat, emissions, wildlife, farms, housing, public data, privacy, Indigenous rights, and long-term community planning. Those impacts may extend far beyond the nearest property line.

If the public is expected to live with those impacts, the public should have a meaningful opportunity to understand, question, challenge, influence, and, where appropriate, oppose the project before key decisions are made.

The public should not ask only:

Was there consultation?

The better question is:

Was the consultation meaningful?

Did residents receive the right information?

Did they receive it early enough?

Was it understandable?

Were key documents public?

Were alternatives still possible?

Could the project change?

Could approval be delayed?

Could conditions be strengthened?

Could the public say no?

Or were residents being asked to respond after the real decisions had already been made?

A meeting is not consent.

A notice is not consent.

A slide deck is not consent.

A public hearing is not meaningful if the outcome is already functionally decided.

Consultation Before Commitment

The timing of consultation matters.

If land has already been assembled, tax incentives negotiated, utility agreements advanced, water access discussed, political announcements made, infrastructure planned, and public agencies aligned behind the project, then public consultation may arrive too late.

The public may still be allowed to speak.

But speaking is not the same as influencing.

A community should be consulted before the project becomes politically, financially, or administratively difficult to stop. Public input should occur while location, scale, design, water use, power demand, ownership structure, public subsidies, emergency planning, and approval conditions are still open to change.

Consultation after commitment is not consent.

It is damage control.

Information Must Be Complete Enough to Respond

Residents cannot evaluate a proposal they cannot understand.

Public consultation should include more than promotional material. The public should receive enough information to assess the project's real impacts, including facility type, full buildout, ownership, operator, tenants or permitted uses, water demand, power demand, infrastructure requirements, tax incentives, emergency risks, environmental impacts, monitoring plans, public costs, and expansion rights.

The information should be specific.

Not "low water use." - How much water?

Not "renewable energy." -What source, what contract, what timing, what grid impact?

Not "minimal noise." -Measured where, at what frequencies, during what conditions?

Not "local jobs." - How many permanent local full-time jobs, at what wages, with what guarantees?

Not "future phases." - How many, how large, and what approvals will they require?

A public process built around vague information produces vague consent.

Plain Language

Technical documents matter, but plain-language explanations matter too.

A proposal may include engineering studies, environmental reports, grid applications, acoustic modelling, water balances, traffic studies, tax agreements, ownership structures, and emergency plans. Those documents may be difficult for ordinary residents to interpret, especially when time is limited.

The public should be given plain-language summaries that accurately explain the technical material without hiding the uncertainty, assumptions, limits, or risks.

Plain language does not mean simplified to the point of uselessness.

It means understandable enough for residents to know what is being proposed, what is uncertain, what is at stake, what choices remain, and what questions they should ask.

If only specialists can understand the project, the consultation process has failed the public.

Access to Documents

Public consultation should be based on documents, not assurances.

Residents should be able to review the studies, agreements, applications, maps, modelling, permits, licences, staff reports, consultant reports, and approval conditions that decision-makers are using.

If key documents are withheld as confidential, commercially sensitive, security-sensitive, incomplete, or not yet finalized, the public should ask whether approval can proceed fairly without them.

Some information may require redaction. Personal information, security details, or narrowly defined confidential material may need protection. But confidentiality should not be used to hide

public costs, water demand, power demand, infrastructure obligations, tax incentives, ownership, environmental impacts, emergency risks, monitoring requirements, or enforceable conditions.

The public should see the evidence before being asked for trust.

Notice Must Reach the Affected Public

Consultation often begins with formal notice rules.

Those rules may be too narrow.

A notice may be mailed only to nearby landowners even though the project affects water systems, grid capacity, roads, taxes, emergency services, agricultural land, public infrastructure, watersheds, wildlife, air quality, sound, and future development across a wider area.

The affected public is not only the people living beside the fence.

It may include residents across the municipality, farmers using the same roads or watershed, Indigenous governments, downstream communities, ratepayers, public service providers, schools, hospitals, care homes, local businesses, emergency responders, utility customers, workers, and future residents.

The public should ask whether notice was designed to meet the minimum legal requirement or to reach everyone meaningfully affected.

A narrow notice area can produce a narrow understanding of public concern.

Accessibility

Consultation should be accessible.

Meetings should be held at times and places people can attend. Documents should be available online and in physical form where needed. Technical materials should be searchable. Plain-language summaries should be provided. Virtual participation should be available where possible. Written submissions should be accepted. People should have enough time to prepare.

Accessibility also means considering disability access, transportation, childcare, language, internet access, hearing or vision needs, rural distance, work schedules, caregiving responsibilities, and the ability of elders, youth, low-income residents, and people with chronic illness to participate.

A public meeting held at an inconvenient time, with dense documents released days before, is not meaningful consultation.

The public should not have to overcome unnecessary barriers to participate in decisions that may affect their lives for decades.

Consultation Is Not Advertising

Public engagement should not be a marketing exercise.

A developer open house may include display boards, renderings, talking points, economic impact numbers, videos, and staff available to answer questions. That can be useful. But it is not enough if the event is designed to persuade rather than listen.

The public should ask whether consultation materials present risks as clearly as benefits.

Do they disclose uncertainty?

Do they identify unresolved issues?

Do they present alternatives?

Do they explain public costs?

Do they distinguish between promised and enforceable benefits?

Do they state what the company is not yet able to answer?

Do they record public concerns accurately?

Do those concerns change anything?

Consultation should not be a performance of openness.

It should be a process for public influence.

The Right to Ask Follow-Up Questions

Public consultation should allow follow-up.

Data center proposals are complex. A resident may not know what to ask until after hearing an answer. A technical response may raise new concerns. A water study may lead to grid questions. A grid answer may raise subsidy questions. A subsidy answer may raise tax questions. A noise report may raise livestock questions. An emergency plan may raise road questions.

A single meeting with limited speaking time is rarely enough.

The public should have a process for submitting written questions, receiving written answers, reviewing those answers, and asking follow-up questions before decisions are made.

Answers should be public.

If one resident asks an important question, the whole community should see the answer.

Meaningful Hearings

A public hearing should be more than a legal checkpoint.

For a hearing to be meaningful, decision-makers must have the ability and willingness to respond to what they hear. They should be able to delay approval, request more information, impose stronger conditions, reject insufficient studies, require new consultation, or refuse approval where warranted.

If decision-makers cannot change the outcome, the hearing is not meaningful.

If the project has already been politically endorsed, financially supported, or publicly celebrated before the hearing, the public may reasonably ask whether the hearing is real.

Decision-makers should enter public hearings with questions, not conclusions.

The Problem of Pre-Approval Momentum

Large projects can build momentum before formal approval.

Announcements may be made. Politicians may praise the investment. Economic development agencies may promote the project. Utilities may begin planning. Land may be cleared or optioned. Staff may spend months negotiating. Grants may be discussed. Road upgrades may enter budgets. Public statements may frame the project as inevitable.

By the time residents are invited to comment, opposing the project may feel like opposing jobs, progress, investment, technology, or the future.

This is not neutral.

Pre-approval momentum can pressure councils, regulators, and residents to accept a project before the evidence is complete.

The public should ask whether decision-makers have kept an open mind or whether public consultation is being used to legitimize a decision already made.

Consent and Indigenous Rights

Public consultation with residents is not the same as consultation with Indigenous governments.

Indigenous governments are rights-holders. Their relationship to land, water, treaty rights, cultural sites, harvesting, governance, data, and future impacts is distinct from general public engagement.

A project may require Indigenous consultation, accommodation, consent, or approval according to applicable laws, treaties, Indigenous legal orders, and the specific rights affected.

Public open houses do not replace Indigenous consultation.

A municipality, province, state, federal agency, utility, or developer should not treat Indigenous rights as one category of public comment. Indigenous governments must be engaged early, respectfully, with full information, adequate time, resources for review, and the ability to influence whether and how the project proceeds.

Consent cannot be presumed because a public meeting occurred.

Consultation With Those Most Affected

The people most affected may be the least able to participate.

Nearby residents may be overwhelmed by technical documents. Farmers may be busy during seasonal work. People with disabilities may face access barriers. Low-income residents may lack time, transport, or internet. Youth may be excluded from formal meetings. Elders may need support. People working shifts may be unable to attend evening hearings. Tenants may fear speaking against landowners or employers. Workers may fear retaliation. Indigenous communities may be asked to respond without adequate resources.

Meaningful consultation should identify who is most affected and remove barriers to participation.

The public process should not favour those with the most time, money, technical knowledge, or political access.

Consultation Records

Consultation should leave a public record.

That record should include notices, meeting materials, attendance, questions asked, answers provided, written submissions, technical responses, unresolved concerns, changes made to the project, and reasons why certain concerns were rejected.

The public should be able to see whether consultation changed the proposal.

If consultation produces no changes, the record should explain why.

A public process that listens but never changes anything should be examined closely.

Public Consent Is Ongoing

Consent is not a single moment.

A data center may change after approval. Tenants may change. Ownership may change. Power demand may increase. Water demand may increase. AI workloads may be added. Backup generators may expand. Public subsidies may change. Future phases may proceed. Monitoring may reveal unexpected impacts. Complaints may increase. Emergencies may occur.

Public consultation should not end at approval.

Major changes should trigger renewed public review. Ongoing monitoring should be public. Complaints should be visible. Annual reporting should be required. Community oversight should continue. Future phases should not proceed on the assumption that the first hearing granted permanent consent for every later version of the project.

The public should not be asked to consent once to a project that can change many times.

Core Questions

Timing

When did public consultation begin?

Had land already been purchased, optioned, or assembled?

Had tax incentives already been negotiated?

Had utility agreements already advanced?

Had water access already been discussed?

Had government officials already publicly endorsed the project?

Had infrastructure planning already begun?

Were key project decisions still open to change?

Could public input affect the location, scale, design, timing, conditions, or approval?

Information Provided

What information was given to the public?

Was the facility type disclosed?

Was full buildout disclosed?

Was ownership disclosed?

Was the operator disclosed?

Were tenants or permitted uses disclosed?

Were water demand, power demand, infrastructure requirements, tax incentives, emergency risks, environmental impacts, monitoring plans, and expansion rights disclosed?

Were uncertainties clearly identified?

Were assumptions disclosed?

Were alternatives presented?

Documents

Were full technical documents released?

Were studies, agreements, permits, licences, maps, staff reports, consultant reports, and draft conditions available?

Were documents released early enough for review?

Were documents searchable and downloadable?

Were plain-language summaries provided?

Were documents withheld?

If documents were withheld, why?

Can redacted versions be released?

Can approval proceed fairly without them?

Notice

Who was notified?

How were they notified?

How far did the notice area extend?

Were residents beyond the immediate property boundary notified?

Were farmers, Indigenous governments, schools, hospitals, care homes, local businesses, emergency services, utility customers, ratepayers, and downstream communities notified where relevant?

Was notice provided in enough time?

Was notice understandable?

Was notice repeated through multiple channels?

Accessibility

Were meetings held at accessible times?

Were meetings held in accessible locations?

Were online options provided?

Were written submissions accepted?

Were documents available in accessible formats?

Were language supports provided where needed?

Were disability accommodations provided?

Were transportation, internet access, work schedules, caregiving responsibilities, and rural distance considered?

Could youth, elders, low-income residents, renters, workers, and people with disabilities participate meaningfully?

Hearings

Was there a formal public hearing?

Could the public ask questions?

Could the public ask follow-up questions?

Were answers given in writing?

Were all answers made public?

Could decision-makers request more information?

Could approval be delayed?

Could conditions be changed?

Could the project be rejected?

Had decision-makers already endorsed the project?

Was the hearing held before or after major commitments were made?

Consultation Quality

Did consultation materials present benefits and risks fairly?
Were public costs disclosed?
Were alternatives discussed?
Were unresolved issues identified?
Were public concerns recorded accurately?
Did public input change the proposal?
Did public input change conditions?
Were reasons given when concerns were rejected?
Was consultation independently facilitated?
Was the process designed to listen or to persuade?

Indigenous Governments

Which Indigenous governments may be affected?
Were they engaged before key decisions were made?
Were they provided full information?
Were they given enough time and resources to review the project?
Were their laws, protocols, and decision-making processes respected?
Were impacts on rights, lands, waters, harvesting, culture, data, and governance assessed?
Did Indigenous concerns change the project?
Was accommodation required?
Was consent required?

Most Affected Communities

Who is most affected by the project?
Were those people specifically consulted?
Were nearby residents consulted?
Were farmers consulted?
Were workers consulted?
Were local businesses consulted?
Were schools, hospitals, care facilities, and public agencies consulted?
Were vulnerable residents consulted?
Were people who rely on the same water source, roads, grid, or emergency services consulted?
Were barriers to participation addressed?

Ongoing Consent

Will future phases require new consultation?
Will tenant changes require public notice?
Will ownership changes require public notice?
Will increased water or power demand require public review?
Will AI, surveillance, crypto mining, or public-sector data uses require public review?

Will monitoring data be public?
Will complaints be reported publicly?
Will annual public meetings be required?
Can the public trigger review after approval?

Red Flags

A consultation process deserves greater scrutiny when the public hears:
"Public consultation requirements have been met."
"The open house was well attended."
"The public had an opportunity to comment."
"Technical documents are available upon request."
"Key agreements are still being finalized."
"Those details will be addressed after approval."
"The project has already received strong government support."
"The hearing is limited to land use."
"Future phases will be consulted on later."
"Public concerns will be considered."

Legal notice is not meaningful consultation.
Attendance is not consent.
Commenting is not influence.
A hearing is not meaningful if key documents are missing.
Consultation after commitment is not public consent.

What Communities Should Ask For

Before approval, communities should ask for:
Early consultation before major commitments are made.
A complete plain-language project summary.
Public release of all key documents.
Enough time for public review.
Accessible meeting formats.
Written question-and-answer processes.
Public answers to public questions.
Disclosure of all uncertainties, assumptions, and unresolved issues.
Disclosure of all public subsidies, utility agreements, water demands, power demands, ownership structures, and expansion rights.
Independent facilitation where trust is low.
Specific outreach to the people and communities most affected.
Separate and appropriate engagement with Indigenous governments as rights-holders.
A consultation record showing what was asked, what was answered, what changed, and what remains unresolved.
A rule that approval cannot proceed until core information is available.

Renewed public consultation for major changes, future phases, tenant changes, ownership changes, increased water or power demand, AI use, surveillance use, or significant new impacts.

A public trigger process allowing residents, Indigenous governments, municipalities, farmers, public agencies, or affected communities to request review after approval.

The Public Interest Standard

No data center should be approved through a consultation process that asks the public to respond after key decisions have already been made.

The public should receive full, clear, timely, accessible information before approval, while the project can still change.

A community cannot meaningfully consent to a project it does not understand.

It cannot meaningfully participate if documents are missing.

It cannot meaningfully influence a decision that has already been made.

It cannot meaningfully trust a process that treats consultation as a box to check rather than a democratic obligation.

If the public is expected to live with the consequences, the public must be given the information, time, access, and power needed to shape the decision.

Part Two - Physical and Environmental Impacts

A data center is often described as digital infrastructure, but its impacts are not digital.

They are physical.

A data center occupies land. It connects to roads. It draws electricity. It may consume water. It produces heat. It requires cooling. It can generate noise, vibration, light, emissions, stormwater runoff, traffic, construction disturbance, and long-term infrastructure demand. It can affect nearby homes, farms, wetlands, forests, waterways, wildlife, livestock, plants, soil, air, emergency services, and the daily life of a community.

The word "cloud" has done a great deal of damage to public understanding.

There is nothing weightless about the cloud. There is nothing invisible about the land it occupies, the water it may use, the power it requires, the generators it tests, the substations it needs, the transmission lines it triggers, the heat it rejects, or the infrastructure it demands.

This part of the handbook is about those physical realities.

It is not enough for a proposal to say that impacts will be "minimal," "manageable," "mitigated," "sustainable," or "consistent with existing regulations." Those words may be useful starting points, but they are not evidence. The public should be able to see the numbers, methods, assumptions, monitoring plans, enforcement mechanisms, and worst-case scenarios behind every claim.

A data center proposal should be evaluated in the real place where it is being built.

That means asking whether the local watershed can support it. Whether the grid can absorb it. Whether the roads are suitable. Whether the noise standards are adequate. Whether nearby homes, farms, animals, and ecosystems have been considered. Whether drought, wildfire, flooding, heat waves, grid stress, and climate change have been included in the analysis. Whether future expansion has been counted. Whether cumulative impacts have been assessed. Whether the public will be able to verify the project's actual performance after approval.

Too often, environmental review treats each impact separately. Water is studied in one report. Power is discussed somewhere else. Noise is modeled under one set of assumptions. Traffic is considered on its own. Wildlife may be reduced to a seasonal survey. Emergency planning may be treated as a technical appendix. Climate risk may be discussed in general language. Public infrastructure may be separated from private development.

But communities experience these impacts together.

A resident does not live beside a "water impact" on Monday, a "noise impact" on Tuesday, and a "grid impact" on Wednesday. A farm does not experience drought separately from power costs, road disruption, construction dust, wildlife displacement, and nighttime noise. A watershed does not care which department approved which permit. An ecosystem does not divide itself according to municipal, provincial, state, federal, corporate, or regulatory boundaries.

The public-interest question is not simply whether each individual impact can be made to fit inside a regulatory box.

The question is whether the total burden of the project is acceptable, understood, enforceable, and honestly disclosed.

Part Two is designed to help communities ask the physical questions before a data center becomes a physical fact.

5 - Water

Water is one of the first questions every community should ask about a data center proposal.

Not because every data center uses the same amount of water. Not because every data center uses the same cooling system. Not because every project will automatically create a water crisis. But because water is not just another input in an industrial process. Water is life, food, health, habitat, agriculture, culture, treaty rights, emergency planning, climate resilience, and community survival.

A data center proposal should never be evaluated only by asking whether water is technically available.

The better question is whether the water use is publicly justified, locally sustainable, legally enforceable, ecologically responsible, and compatible with the needs of the community, watershed, farms, animals, plants, and future generations.

Data centers may use water directly for cooling. They may use water indirectly through the electricity required to power them. They may require water during construction. They may use water for humidification, fire suppression, cleaning, landscaping, dust control, emergency systems, or other operational needs. They may discharge heated water, treated water, chemically affected water, stormwater, or wastewater. They may rely on municipal water, groundwater, surface water, reclaimed water, industrial wastewater, or private wells.

The public should know which of these apply before approval is granted.

The Problem With "Low Water" Claims

Data center water claims are often presented in ways that sound simple but are not.

A proposal may say the facility will use "minimal water," "low-water cooling," "closed-loop cooling," "air cooling," "water-efficient technology," "reclaimed water," or "best available systems." These phrases may be true in one sense and incomplete in another.

A closed system does not necessarily mean no water use.

A closed-loop cooling system may reduce ongoing water consumption compared with some evaporative systems, but it can still require water for filling, treatment, maintenance, flushing, cleaning, emergency operation, humidification, fire suppression, or heat exchange support. It may still create discharge. It may still use chemicals. It may still require blowdown, wastewater handling, or periodic replacement of fluids. It may still depend on electricity generated by water-intensive power sources elsewhere.

Similarly, a proposal that says it will not use potable water may still affect the watershed. Reclaimed water, wastewater, surface water, groundwater, industrial reuse water, and stormwater are not free of public consequence. Each may already have a role in the local water cycle, agriculture, downstream flows, wetlands, aquifer recharge, ecosystem health, or future municipal planning.

The public should not accept "closed," "efficient," "recycled," or "low-water" as substitutes for actual numbers.

The questions remain:

How much water will be withdrawn?
How much will be consumed?
How much will be returned?
What will be discharged?
Where will it come from?
Where will it go?
What will be in it?
Who will monitor it?
Who will enforce the limits?
What happens during drought, heat waves, equipment failure, wildfire, or grid stress?

Withdrawal, Consumption, and Discharge

Water discussions often become confusing because different terms are used as if they mean the same thing.

They do not.

Withdrawal refers to the amount of water taken from a source.

Consumption refers to the amount of water not returned to that source because it is evaporated, incorporated into a process, removed from the watershed, or otherwise unavailable for immediate reuse.

Discharge refers to water released from the site after use, treatment, contact with equipment, heating, cooling, stormwater collection, or other processes.

A data center could withdraw a large amount of water but return much of it. Another facility could withdraw less water but consume a high percentage through evaporation. Another could use little operational water but discharge stormwater, wastewater, heated water, or chemically treated water in ways that still matter.

The public should not be forced to guess which situation applies.

Every proposal should disclose withdrawal, consumption, and discharge separately. These numbers should be provided by day, month, season, and year, not only as an annual average. Seasonal variation matters because the highest water demand may occur during the hottest, driest periods when communities, farms, rivers, wetlands, wildlife, and emergency services are already under stress.

The Source Matters

It is not enough to ask how much water a data center will use. The public must also ask where the water will come from.

Municipal drinking water raises different concerns than reclaimed wastewater. Groundwater raises different concerns than river withdrawal. Surface water raises different concerns than industrial reuse. Private wells raise different concerns than a regional water system. Water imported from outside the watershed raises different concerns than water drawn locally.

Each source carries public consequences.

If municipal water is used, will households, schools, hospitals, farms, small businesses, parks, and future housing compete with the data center for capacity?

If groundwater is used, what is known about aquifer recharge, existing well users, drought sensitivity, contamination risk, and long-term drawdown?

If surface water is used, how will withdrawals affect streamflow, wetlands, fish, riparian habitat, aquatic species, downstream users, and water temperature?

If reclaimed water is used, what was that water previously used for, and what ecological or municipal function will be lost when it is redirected?

If industrial wastewater is used, what treatment is required, what contaminants may remain, and what happens to the resulting discharge?

If stormwater is captured, how will that affect drainage, flooding, groundwater recharge, wetlands, and downstream flows?

Water is not made harmless simply because it is labelled non-potable.

Drought and Climate Stress

A water assessment that only looks at normal years is not enough.

Communities need to know how the data center will operate during drought, water restrictions, heat waves, wildfires, low river flows, aquifer stress, power shortages, or emergency conditions. These are not hypothetical concerns. Climate change is making water planning more uncertain in many regions, and infrastructure decisions made today may create obligations that last for decades.

The public should ask whether the project's water demand has been tested against worst-case and future-case scenarios, not only historical averages.

What happens if there is a multi-year drought?

What happens if municipal water restrictions are imposed?

What happens if farmers are asked to reduce water use?

What happens if river flows fall below ecological thresholds?

What happens if groundwater levels decline?

What happens if wildfire or extreme heat increases cooling demand?

What happens if the data center has a contractual right to water that competes with emergency public needs?

A data center should not receive water security that the surrounding community does not have.

Water Rights, Priority, and Public Control

The public should know what legal rights the data center will receive.

Will the facility hold a water licence, permit, allocation, contract, utility agreement, or private withdrawal right? How long will that right last? Can it be transferred if the company sells the facility? Can it be expanded later? Can it be reduced during drought? Can it be suspended during emergency conditions? Does the agreement give the company priority over other users?

Water agreements should not be hidden behind commercial confidentiality when they affect public resources.

If a data center is granted long-term access to water, the public should know what has been promised, what limits apply, and whether future councils, residents, farmers, Indigenous governments, or downstream communities will be bound by decisions made today.

Indigenous Rights and Watershed Governance

Water is not only a municipal resource or an industrial input.

In many places, water is connected to Indigenous rights, treaty rights, harvesting rights, cultural responsibilities, sacred sites, traditional land use, fisheries, medicines, food systems, and intergenerational obligations.

A data center proposal should not treat water consultation as a narrow technical exercise. If withdrawals, discharges, infrastructure, land disturbance, aquifer impacts, or watershed changes may affect Indigenous rights or responsibilities, then Indigenous governments and communities must be involved early, meaningfully, and with access to the information required to assess the proposal.

The public-interest question is not only whether a permit can be issued.

It is whether the water decision respects the people, rights, laws, relationships, and ecosystems connected to that water.

Water Quality and Discharge

A data center may affect water not only by using it, but by changing it.

Water may leave the site warmer than it entered. It may contain treatment chemicals, corrosion inhibitors, biocides, cleaning agents, suspended solids, fuel residues, metals, salts, fire suppression chemicals, or other contaminants depending on the systems used. Stormwater may collect pollutants from roofs, roads, parking areas, fuel storage, generators, transformers, construction zones, and industrial surfaces.

The public should ask what water will leave the site, how it will be treated, where it will go, and how it will be monitored.

A discharge should not be considered safe simply because it meets a minimum permit threshold. The community should also ask whether the discharge is appropriate for the receiving environment, whether cumulative impacts have been assessed, whether low-flow conditions were considered, whether thermal impacts were modeled, and whether downstream users and ecosystems were included.

Construction Water

Water use does not begin when servers go live.

Construction may require water for dust suppression, concrete, soil compaction, equipment cleaning, worker facilities, landscaping, fire protection, and site preparation. Construction may also affect stormwater, sediment, wetlands, drainage patterns, shallow groundwater, and nearby wells.

If the project is large or phased, construction impacts may continue for years.

A proposal should disclose construction water needs separately from operational water needs. It should also identify how construction runoff, erosion, sediment, spills, and temporary discharges will be prevented, monitored, and enforced.

The Hidden Water in Electricity

Even a data center that uses little water on site may still be connected to water use elsewhere.

Electricity generation can require water, depending on the source. Thermal power plants may use water for cooling. Hydroelectric systems are directly tied to river flows, reservoirs, fish habitat, downstream ecosystems, and Indigenous rights. Fuel extraction and processing may also involve water impacts. Transmission and new generation projects may affect wetlands, rivers, land, wildlife, and communities.

For that reason, "low on-site water use" should not end the water conversation.

The public should ask whether the facility's electricity demand will increase water use elsewhere in the energy system, especially if new generation, grid expansion, or fossil-fuel backup is required.

Core Questions

Water Demand

How much water will the facility withdraw each day?
How much water will the facility consume each day?
How much water will the facility discharge each day?
What are the projected monthly, seasonal, and annual water figures?
What is the expected water use during peak summer heat?
What is the expected water use during drought?
What is the expected water use during emergency operation?
Are the figures based on the first phase only or the maximum buildout?
Will later phases require new water approvals?
Can water use increase without another public hearing?

Water Source

What is the water source?
Will the facility use municipal drinking water?
Will it use groundwater?
Will it use surface water from a river, lake, reservoir, wetland, or other source?
Will it use reclaimed wastewater, industrial wastewater, stormwater, or non-potable water?
Who else currently relies on that water source?
What is the current condition of the watershed or aquifer?

Is the water source already stressed, overallocated, contaminated, drought-sensitive, or needed for future municipal growth?

Will the project compete with households, farms, local businesses, ecosystems, Indigenous rights, emergency services, or future housing?

Cooling System

What cooling system will be used?
Will the system use evaporative cooling?
Will the system use closed-loop cooling?

Will the system use air cooling?

Will the system use hybrid cooling?

Will the cooling system require water for filling, maintenance, treatment, flushing, cleaning, emergency operation, humidification, or fire suppression?

Will the cooling system create blowdown, wastewater, or other discharge?

What chemicals will be used in the cooling system?

How often will water or cooling fluids need to be replaced?

What happens if the cooling system fails during extreme heat or grid stress?

Closed-System Claims

When the proposal says "closed loop" or "closed system," what exactly is closed?

Does "closed" refer only to the cooling loop, or to the entire facility's water use?

How much initial water is required to fill the system?

How much makeup water will be required over time?

Will any water be discharged from maintenance, flushing, cleaning, treatment, or system replacement?

Will any chemical treatment be used?

Will the system require wastewater handling?

Will the facility still use water for humidification, fire suppression, landscaping, cleaning, construction, or emergency operation?

Will the public receive actual water-use numbers rather than general descriptions?

Discharge and Water Quality

Will the facility discharge water?

Where will discharged water go?

Will discharge enter a municipal sewer system, stormwater system, river, lake, wetland, groundwater system, industrial treatment facility, or other receiving environment?

What temperature will discharged water be?

Will discharge contain chemicals, salts, metals, biocides, corrosion inhibitors, suspended solids, fuel residues, fire suppression chemicals, or other contaminants?

How will discharge be treated?

Who will monitor the discharge?

How often will monitoring occur?

Will results be publicly available?

What enforcement applies if limits are exceeded?

Drought and Emergency Conditions

What happens during drought?

Can the facility be required to reduce water use during water restrictions?

Will the facility have priority access to water?

Can water rights, contracts, or licences be suspended during emergencies?

Will the facility use more water during heat waves?

Will the facility store water on site?

Will emergency water needs affect firefighting, hospitals, homes, farms, or other public priorities?

Has the project been evaluated under future climate scenarios rather than only past averages?

Public Cost and Infrastructure

Will new water infrastructure be required?

Will new wells, pipes, pumps, reservoirs, treatment systems, sewer capacity, stormwater systems, or discharge infrastructure be needed?

Who will pay for those upgrades?

Will the upgrades primarily benefit the data center or the broader community?

Will municipal water or sewer rates increase?

Will the project use capacity that was intended for future housing, agriculture, public services, or local businesses?

Will the water infrastructure be sized for the current project or future expansion?

Monitoring and Accountability

Will actual water use be reported publicly?

Will water withdrawal, consumption, and discharge be reported separately?

Will reporting be real-time, monthly, seasonal, or annual?

Will the public be able to compare actual use against approved limits?

Who verifies the data?

Are reports independently audited?

What penalties apply if the facility exceeds water limits?

Can permits be revised, reduced, suspended, or revoked if impacts are greater than promised?

Red Flags

A water proposal deserves greater scrutiny when the public hears:

"The facility will use minimal water."

"The system is closed loop."

"The project will use non-potable water."

"Water use will be negligible."

"Cooling details will be finalized later."

"Exact water use depends on future tenants."

"Water demand is commercially sensitive."

"The project will use best available technology."

"The facility will not affect local water users."

"Water impacts will be managed through standard permitting."

"The project will use reclaimed water, so there is no impact."

"Annual average water use is low."

"Drought conditions are not expected to be a problem."

What Communities Should Ask For

Before approval, communities should ask for:

A full water balance for the project.

Separate figures for withdrawal, consumption, and discharge.

Daily, monthly, seasonal, annual, peak-demand, and drought-scenario estimates.

Water use figures for each phase and maximum buildout.

Identification of all water sources.

Identification of all discharge locations.

A description of the cooling system.

A plain-language explanation of any closed-loop or closed-system claim.

A list of all chemicals used in cooling, treatment, cleaning, fire suppression, and maintenance.

A construction water plan.

A drought and emergency water plan.

A climate-adjusted watershed or aquifer assessment.

A water infrastructure cost report.

A public reporting and monitoring plan.

An enforcement plan with clear penalties and remedies.

Disclosure of all water licences, contracts, utility agreements, allocations, or priority rights connected to the project.

Evidence of meaningful consultation with Indigenous governments and affected downstream communities where rights, watersheds, ecosystems, or traditional uses may be affected.

The Public Interest Standard

No data center should be approved until the public knows where its water will come from, how much it will withdraw, how much it will consume, what it will discharge, what infrastructure it requires, what happens during drought, and who has the power to enforce limits if promises are broken.

A community should not be asked to trade uncertain water security for vague promises of digital progress.

Water is not a technical footnote.

It is the first measure of whether a data center proposal understands the place where it wants to land.

6 - Electricity and Grid Burden

A data center is not only a building.

It is a major electrical demand.

Every server, cooling system, pump, fan, transformer, security system, lighting system, battery unit, backup generator, and network device requires power. For larger facilities, that demand can be enormous. A single hyperscale data center or data center campus may require as much electricity as a town, a city district, or a major industrial facility.

That demand does not exist in isolation.

It lands on a power grid that may already be aging, constrained, underbuilt, undermaintained, dependent on fossil fuels, vulnerable to extreme weather, or struggling to keep pace with population growth, electrification, housing demand, industry, agriculture, hospitals, schools, small businesses, and climate adaptation.

For this reason, the public should not ask only whether a data center can be connected to the grid.

The better question is whether the data center can be connected without weakening the public interest.

Will the project require new generation?

Will it require new transmission lines?

Will it require new substations, transformers, distribution upgrades, battery systems, or backup generation?

Will residents and businesses pay higher rates because of it?

Will public infrastructure be built primarily for private growth?

Will the facility increase fossil fuel use, even while claiming to be powered by renewables?

Will local communities carry the burden while distant companies receive the benefit?

Electricity is not an invisible input. It is a public system, a public cost, a public vulnerability, and in many places, a public resource.

The Grid Is Not a Blank Plug

Data center proposals often speak of electricity as though it is simply available.

It is not.

Electricity has to be generated, transmitted, distributed, balanced, backed up, regulated, financed, maintained, and delivered in real time. A large new load can affect the grid far beyond the project site. It may require new wires, substations, transformers, grid studies, reserve capacity, demand management, backup systems, or new generation. It may increase pressure on utility planning. It may affect reliability during extreme heat, extreme cold, wildfire, drought, storms, or peak demand periods.

A data center may be described as private investment, but the grid it depends on is usually a shared system. When a large private user connects to that system, the public has the right to know whether the private user is paying the full cost of the demand it creates.

A project should not be allowed to look affordable by quietly shifting grid costs onto households, farms, small businesses, municipalities, schools, hospitals, or future ratepayers.

Power Demand Must Be Disclosed Clearly

The first electrical question is simple:

How much power will the facility require?

The answer should not be hidden behind vague language such as "high-efficiency operations," "green computing," "AI-ready infrastructure," or "sustainable digital services." The public needs real numbers.

Power demand should be disclosed in megawatts for the first phase, each later phase, and the maximum buildout. It should include computing equipment, cooling, pumps, fans, lighting, security, battery systems, network systems, auxiliary equipment, and all supporting infrastructure.

The public should also know whether the stated demand is an average, a peak, a contracted maximum, or only an estimate. A facility that averages one level of demand may still require the grid to reserve capacity for much higher peaks. That reserved capacity can shape utility planning, infrastructure costs, and reliability.

The project should also disclose whether it can increase power demand later without returning for public review.

A community cannot evaluate a project if it is told only what the first building might require while the approval allows a much larger future campus.

Transmission, Substations, and Grid Upgrades

A data center may require more than a connection.

It may require a new substation. It may require new transmission lines. It may require upgraded transformers, distribution lines, switching equipment, rights-of-way, roads, vegetation clearing, land acquisitions, battery systems, control systems, or grid reinforcement many kilometres away from the site.

These upgrades matter because they may create new land impacts, new costs, new maintenance obligations, and new development pathways.

A transmission line built for one data center may later enable additional industrial development. A substation built for one project may become the anchor for a data center corridor. A grid upgrade described as necessary for one proposal may become the public-funded foundation for many more.

The public should ask whether grid infrastructure is being sized only for the proposed project, or whether it is being oversized for future phases, future data centers, or broader industrial expansion.

If the infrastructure is larger than the current proposal requires, the public should know who requested that capacity, who pays for it, who benefits from it, and whether it commits the community to a larger development pattern.

Ratepayer Costs and Public Subsidy

Electricity costs can be shifted in ways that are not obvious.

A data center may pay for its direct connection, while broader grid upgrades are paid for through utility rates. It may receive discounted power, interruptible rates, industrial tariffs, tax incentives,

infrastructure grants, or special agreements. It may be treated as an economic development project, while the public absorbs costs through higher rates, deferred maintenance, public debt, municipal servicing, or utility-wide cost recovery.

The question is not only what the company pays.

The question is what the public pays.

If a data center requires new electrical infrastructure, the full cost should be disclosed before approval. That accounting should include direct connection costs, upstream grid upgrades, transmission expansion, distribution upgrades, new generation, reserve capacity, backup systems, regulatory costs, land acquisition, maintenance, and any public subsidy or discount.

The public should also know whether local residents and businesses will face higher electricity rates because of the project.

No community should be asked to subsidize private digital infrastructure through bills that arrive quietly years later.

Grid Reliability and Public Priority

A data center can be a constant, high-demand electrical user.

That can matter during peak demand, extreme weather, wildfire, drought, equipment failure, fuel shortages, or grid emergencies. If the grid is stressed, the public needs to know who gets priority and who is expected to reduce demand.

Will the data center be required to curtail operations during emergencies?

Will it participate in demand-response programs?

Can it be disconnected or reduced during grid stress?

Will it have a contractual right to power even when households, farms, hospitals, schools, or small businesses are being asked to conserve?

Will backup systems allow the facility to continue operating while nearby communities experience outages?

A data center should not receive a level of power security that weakens public resilience.

If a facility is treated as critical infrastructure, the public should know why. If it is not critical infrastructure, the public should know why it should receive priority access to shared grid capacity.

Fossil Backup and Hidden Emissions

A data center may claim to be powered by renewable energy while still relying on fossil backup.

Backup systems can include diesel generators, natural gas turbines, fuel storage, emergency generators, or other on-site systems. These systems may be tested regularly. They may run during outages, grid emergencies, maintenance, or peak demand events. They may produce air pollution, noise, greenhouse gas emissions, fuel spill risks, fire risks, and emergency response burdens.

The public should ask how many backup generators will be installed, what fuel they will use, how often they will be tested, how long they can run, where fuel will be stored, what emissions they produce, and whether nearby residents, schools, farms, animals, and ecosystems have been considered.

A renewable claim does not erase backup emissions.

Nor does a renewable power purchase agreement necessarily mean the facility is physically powered by renewable electricity every hour it operates.

Renewable Claims Must Be Specific

Data center proposals often rely on phrases such as "powered by renewable energy," "net zero," "carbon neutral," "green power," "sustainable operations," or "matched with clean energy."

These claims should be examined carefully.

The public should ask whether the facility will receive renewable electricity directly, whether it will buy credits, whether it will sign a power purchase agreement, whether the renewable energy is new or existing, whether the claim is annual or hourly, and whether fossil power is still used when renewable generation is unavailable.

A facility may claim to offset its annual electricity use while still drawing power from a fossil-heavy grid during peak demand. It may purchase renewable certificates without adding new clean generation. It may rely on renewable projects located far from the community bearing the local grid impacts. It may describe itself as clean while causing new fossil generation, grid reinforcement, or backup emissions elsewhere.

The public should not accept renewable language without asking what it means in physical, legal, and operational terms.

Alternative Energy and Lower-Impact Power Options

Before a data center is approved, the public should ask whether lower-impact power options were seriously assessed.

If solar energy is considered viable enough to power proposed space-based data centers, it should at least be examined for terrestrial facilities. That does not mean rooftop or on-site solar can power every data center by itself. Large data centers often require constant power, while solar generation varies by daylight, weather, season, and location. But variability is not a reason to avoid the question. It is a reason to ask how solar, storage, demand management, off-site renewables, waste heat use, and facility design could reduce the burden on the grid.

The public should ask whether the developer assessed on-site solar, nearby solar, wind, geothermal, waste heat recovery, district energy systems, battery storage, thermal storage, demand response, colocating near surplus renewable generation, using curtailed renewable power, or scaling the project to available clean energy rather than forcing the grid to expand around the project.

A company proposing a large data center should not be allowed to treat the public grid as the default solution while dismissing alternatives as inconvenient.

The question is not whether alternative energy can solve every problem.

The question is whether the developer has made every reasonable effort to reduce the public burden before asking the community, utility, ratepayers, and environment to carry it.

Battery Storage

Battery storage may reduce some grid impacts, but it also creates its own questions.

Batteries may help manage peak demand, provide backup power, participate in grid services, reduce generator use, or improve resilience. But battery systems also require land, materials, fire

planning, emergency response capacity, cooling, monitoring, replacement, recycling, and safety protocols.

The public should know whether batteries are being used to reduce public grid burden or merely to protect the data center from outages. It should also know whether battery systems create fire, smoke, toxic release, water use, waste, or emergency response risks.

Battery storage should not be treated as a magic word. It is infrastructure, and it must be evaluated as infrastructure.

Behind-the-Meter Power and Private Generation

Some data centers may propose their own power generation.

This can include solar farms, wind projects, gas plants, fuel cells, geothermal systems, small modular reactors, hydrogen systems, or other behind-the-meter arrangements. These systems may reduce some grid reliance, but they can also create new land impacts, water impacts, emissions, waste issues, safety concerns, fuel supply chains, and regulatory questions.

The public should ask whether private generation serves the public interest or simply creates a private energy system for private digital growth.

If a data center builds its own power source, the community should know what fuel is used, where the energy comes from, what emissions are created, what land is affected, what water is required, what waste is produced, what emergency risks exist, and whether the project will still rely on the public grid during shortages or failures.

Energy Efficiency Is Not the Same as Low Impact

A data center may be more efficient than older facilities and still consume enormous amounts of electricity.

Efficiency matters, but it must not be used to obscure scale. A highly efficient facility can still create major grid burden if it is very large. A project can have an impressive power usage effectiveness score and still require new generation, transmission upgrades, backup generators, water-intensive cooling, and public subsidies.

The public should ask not only how efficient the facility is, but how much total power it will use.

A smaller inefficient facility and a massive efficient facility are not the same public-interest question. Scale matters.

Core Questions

Power Demand

What is the projected electrical demand of the project in megawatts?

What is the demand for the first phase?

What is the demand for each later phase?

What is the maximum buildout demand?

Are the figures average demand, peak demand, contracted capacity, or estimated operational use?

How much of the demand is for computing equipment?

How much is for cooling?

How much is for pumps, fans, lighting, security, networking, batteries, and supporting systems?

Can the facility increase its power demand later without new public approval?

Will electricity demand vary by season, heat waves, workload, tenant, or AI use?

Grid Capacity

Can the existing grid support the project without upgrades?

What grid studies have been completed?

Will the project require new transmission lines?

Will it require a new substation?

Will it require transformer upgrades?

Will it require distribution upgrades?

Will it require new generation?

Will it require battery storage, grid controls, reserve capacity, or other system changes?

Are upgrades required only at the project site, or elsewhere in the grid?

Will upgrades affect other communities, landowners, farms, ecosystems, or Indigenous rights?

Cost and Ratepayer Burden

Who pays for the direct electrical connection?

Who pays for upstream transmission upgrades?

Who pays for substations, transformers, distribution upgrades, land acquisition, vegetation clearing, maintenance, and regulatory costs?

Will any costs be recovered through utility rates?

Will residential, farm, municipal, school, hospital, or small business ratepayers pay more because of this project?

Will the data center receive discounted power, special tariffs, industrial rates, tax incentives, grants, or other public support?

Will the developer pay the full cost of the grid burden it creates?

Has a full public cost-benefit analysis been completed?

Reliability and Curtailment

Will the project affect grid reliability?

Will it increase risk during peak demand?

Will it increase risk during extreme heat, extreme cold, wildfire, drought, storms, or grid emergencies?

Can the facility be required to reduce demand during grid stress?

Will the facility participate in demand-response programs?

Will it have interruptible service?

Will it have priority access to electricity?

Could local residents or businesses be asked to conserve while the data center continues operating?

What happens if the facility's power demand exceeds projections?

Renewable Energy Claims

What does "renewable powered" mean in this proposal?

Will renewable electricity be delivered directly to the facility?

Will the facility use renewable energy certificates or credits?

Is the renewable energy new or existing?

Is the energy matched hourly, daily, monthly, or annually?

Will fossil power be used when renewable generation is unavailable?

Will the project require new fossil generation, backup generation, or grid firming?

Are renewable claims legally enforceable?

Will renewable energy used by the data center reduce clean energy available for homes, businesses, public services, or other climate goals?

Alternative Energy Assessment

Were lower-impact power options assessed before the grid connection was requested?

Was on-site solar assessed?

Was off-site solar assessed?

Was wind assessed?

Was geothermal assessed?

Was waste heat recovery assessed?

Was district energy integration assessed?

Was battery storage assessed?

Was thermal storage assessed?

Was demand response assessed?

Was colocating near surplus or curtailed renewable energy assessed?

Was reducing the project scale assessed?

Was phased development tied to available clean energy assessed?

If alternatives were rejected, what reasons were given, and are those reasons public?

Backup Power

What backup power systems will be used?

How many diesel generators, gas turbines, batteries, fuel cells, or other backup systems will be installed?

What fuels will be stored on site?

How much fuel will be stored?

How often will backup systems be tested?

How long can they run?

What emissions will they produce during testing and emergencies?

What noise will they produce?

What fire, spill, explosion, smoke, or hazardous-material risks exist?
Who monitors backup-system emissions and safety?

Battery Storage

Will battery storage be installed?
What type of batteries will be used?
What is the storage capacity?
Will batteries reduce grid burden or only provide backup for the data center?
What fire safety systems are required?
What emergency response training is required?
What water, chemicals, or fire suppression materials may be needed during a battery incident?
How will batteries be replaced, recycled, or disposed of?
Who is responsible for long-term battery waste?

Private or Behind-the-Meter Generation

Will the data center build or contract dedicated power generation?
What type of generation?
Where will it be located?
What land, water, emissions, waste, fuel, safety, and transmission impacts will it create?
Will the facility still rely on the public grid?
Will private generation be regulated as critical energy infrastructure?
Will excess power be available to the public grid, or reserved for private use?

Efficiency and Total Load

What is the facility's expected power usage effectiveness?
How was that figure calculated?
Is it based on design assumptions or verified operations?
Will efficiency data be reported publicly?
How much total electricity will the facility use even after efficiency measures?
Will efficiency claims be enforceable?
Can the facility be penalized if actual performance is worse than promised?

Red Flags

An electricity proposal deserves greater scrutiny when the public hears:
"The facility will be powered by renewable energy."
"The project will be net zero."
"The grid can accommodate the load."
"Upgrades will be handled by the utility."
"Power details are commercially sensitive."
"The project will use best available technology."
"The facility will be highly efficient."

"Backup generators are only for emergencies."
"The project will create clean digital infrastructure."
"Energy use depends on future tenants."
"The development will be AI-ready."
"The project will not affect local ratepayers."
"Costs will be recovered through standard utility processes."
"The company will purchase clean energy credits."

What Communities Should Ask For

Before approval, communities should ask for:
A full electricity demand forecast.
Demand figures for the first phase, each later phase, and maximum buildout.
Average and peak demand estimates.
A public grid capacity study.
A list of all required transmission, substation, transformer, distribution, and generation upgrades.
A full accounting of who pays for each grid upgrade.
A ratepayer impact assessment.
A reliability and emergency operations assessment.
A curtailment and demand-response plan.
A renewable energy plan with clear definitions and enforceable commitments.
An alternative energy assessment.
A backup power plan.
A battery storage safety plan, if applicable.
A private generation assessment, if applicable.
A public reporting plan for electricity use, efficiency, emissions, backup generator testing, and grid impacts.
Disclosure of all electricity contracts, special tariffs, subsidies, discounts, grants, or public financial supports connected to the project, except for narrowly justified confidential details.

The Public Interest Standard

No data center should be approved until the public knows how much electricity it will require, whether the existing grid can support it, what upgrades are needed, who will pay for them, what backup systems will be used, whether renewable claims are real, and whether lower-impact alternatives were seriously assessed.

A community should not be asked to carry private digital growth on a public electrical system without knowing the cost.

The grid is not just a plug.

It is shared infrastructure. It is public vulnerability. It is household bills, farm operations, hospitals, schools, small businesses, emergency services, climate planning, and future growth.

Before a data center is connected, the public has the right to ask whether the connection serves the public interest.

7 - Land Use and Community Fit

A data center is not suitable everywhere simply because land is available.

Land is never just empty space. It may be farmland, wetland, forest, grassland, habitat, watershed, floodplain, cultural landscape, traditional territory, wildlife corridor, future housing area, transportation route, agricultural buffer, or open space that gives a community room to breathe and grow.

A data center proposal should therefore be evaluated not only as an economic development opportunity, but as a land-use decision with long-term consequences.

Once a data center is built, it may shape the surrounding area for decades. It may require roads, substations, transmission lines, fencing, security lighting, water infrastructure, sewer systems, stormwater controls, fuel storage, backup generators, cooling equipment, and emergency access. It may introduce industrial-scale infrastructure into places that were previously rural, agricultural, ecological, residential, or undeveloped.

The public should ask whether the proposed site is appropriate for the scale, demands, risks, and long-term footprint of the facility.

The question is not only:

Can it be built here?

The better question is:

Should this kind of infrastructure be built here?

Community Fit Is Not Static

A project may appear compatible when it is approved because it is located on the edge of a municipality, near open land, beside farmland, or outside an existing residential area. But communities change. Housing expands. Schools are built. Hospitals and care facilities are added. Industrial parks grow. Roads become busier. Farmland is subdivided. Open space disappears. What seems isolated today may become surrounded tomorrow.

For this reason, land-use review must consider future community fit, not just current community fit.

A data center should be evaluated against existing land uses, approved future land uses, likely development patterns, municipal growth plans, housing needs, transportation plans, climate adaptation plans, and long-term regional development. If the facility is expected to operate for decades, then the approval process should ask what the surrounding community may look like in ten, twenty, thirty, or forty years.

A data center placed in open space today may become a permanent industrial island inside a future residential or mixed-use area. A site that currently appears distant from people may later sit near homes, schools, playgrounds, seniors' housing, medical facilities, farms, parks, trails, or public gathering spaces.

The public should not be told that impacts are acceptable simply because few people live nearby at the time of approval.

Land-use decisions create the future conditions that later communities must live with.

Farmland and Food Systems

Agricultural land should not be treated as vacant land simply because it is not covered in buildings.

Farmland is infrastructure. It produces food, supports rural economies, stores knowledge, sustains families, preserves soil, manages water, supports pollinators, and forms part of a region's long-term resilience. Once high-quality farmland is converted to industrial infrastructure, it may be difficult or impossible to restore.

A data center proposal on or near farmland should be assessed for direct land loss, fragmentation of farm operations, impacts on irrigation, drainage, access roads, dust, noise, light, traffic, water competition, power costs, soil compaction, and conflicts with livestock or crop production.

A data center proposal on agricultural land should be required to answer a higher standard of public-interest review. Why must this project use land capable of producing food? What non-agricultural sites were considered first? Are brownfields, already-industrial land, degraded sites, or lower-value development lands available? What is lost if this land is removed from agriculture permanently?

The question should not be whether farmland can be converted.

The question should be whether it should be.

.

Wetlands, Forests, Grasslands, and Natural Areas

Wetlands, forests, grasslands, riparian zones, and natural areas are not empty or idle land.

They filter water, store carbon, reduce flooding, recharge groundwater, cool local environments, provide habitat, support pollinators, protect biodiversity, and help communities adapt to climate change. They may also hold cultural, spiritual, recreational, and educational value.

A data center proposal should identify whether the site affects wetlands, streams, ponds, floodplains, forests, native grasslands, wildlife habitat, riparian corridors, aquifer recharge areas, or ecologically sensitive land.

The review should consider not only the building footprint, but the full disturbance area: roads, substations, fencing, transmission lines, stormwater ponds, drainage changes, parking, construction staging, lighting, noise, dust, vegetation clearing, and future expansion.

A project that avoids a wetland on paper may still harm it through altered drainage, runoff, heat, sediment, pollutants, groundwater changes, or loss of surrounding habitat.

Housing Proximity and Human Health

Data centers may operate continuously. That makes proximity to housing especially important.

Residents may be affected by construction noise, truck traffic, nighttime lighting, backup generator testing, cooling equipment, low-frequency sound, vibration, air emissions, road changes, emergency risks, and changes to community character.

A facility that seems acceptable in an industrial area may raise different concerns if it is near homes, apartments, mobile home communities, seniors' residences, shelters, worker housing, or future residential growth areas.

The public should ask whether proper setbacks have been established, whether the setbacks reflect real-world operations, and whether they account for future residential development around the site.

It is not enough to ask whether existing homes are far enough away. The approval should also ask whether future homes should ever be allowed near the facility, and whether the facility's presence will limit the community's ability to grow safely and comfortably.

Schools, Hospitals, Care Facilities, and Vulnerable Populations

Some land uses require greater protection.

Schools, daycares, hospitals, clinics, long-term care homes, seniors' housing, disability services, shelters, playgrounds, recreation areas, and community gathering places should be considered carefully when evaluating a data center site.

Children, seniors, patients, people with disabilities, people with respiratory conditions, people sensitive to noise, and people who cannot easily relocate may be more affected by noise, light, air emissions, traffic, emergency events, and disrupted public services.

A data center proposal should identify all sensitive sites near the facility, along transportation routes, and in areas that may be affected by emergency planning, power infrastructure, water infrastructure, or future expansion.

The public should ask whether the site creates avoidable burdens for people with the least ability to avoid them.

Wildlife Corridors and Habitat Connectivity

Wildlife does not move according to zoning maps.

A data center may disrupt wildlife corridors through fencing, roads, lighting, noise, habitat loss, vegetation clearing, water changes, traffic, and human activity. Even when the building footprint is limited, the supporting infrastructure may fragment habitat or alter movement patterns.

The public should ask whether the site sits in or near migration routes, breeding areas, nesting habitat, riparian corridors, wetlands, forest edges, grasslands, pollinator habitat, amphibian movement areas, or other ecological connections.

The review should include cumulative habitat fragmentation, not only direct habitat removal.

A wildlife corridor narrowed by one project may be broken by the next.

Transportation Routes and Construction Access

Data centers can generate significant construction traffic.

Even if permanent staffing is low, construction may involve heavy equipment, concrete trucks, steel deliveries, fuel deliveries, electrical equipment, transformers, cooling systems, backup generators, fencing, roadwork, and utility installation. Large transformers and mechanical systems may require special routes, bridge assessments, road widening, turning-radius changes, escort vehicles, or temporary closures.

Once operational, the facility may still require maintenance traffic, security traffic, fuel deliveries, generator service, equipment replacement, waste removal, emergency access, and snow or storm response.

The public should ask whether local roads, bridges, intersections, and rural routes can handle the project safely without shifting costs or risks onto residents.

Transportation review should include school bus routes, farm equipment routes, emergency response routes, pedestrian routes, cycling routes, public transit, local businesses, and seasonal road conditions.

Security, Fencing, and Community Character

Data centers often require security.

That may include fencing, cameras, gates, lighting, barriers, guards, restricted access roads, and surveillance systems. These may be appropriate for the facility, but they also change how land feels and functions in a community.

A large fenced and secured site can sever informal pathways, block views, alter rural character, reduce public access, create visual intrusion, and signal a shift from open or mixed-use land to restricted industrial territory.

The public should ask whether the design fits the community, whether visual screening is adequate, whether lighting is controlled, whether public access is affected, and whether the facility creates a hardened landscape where a more compatible land use could have existed.

Future Expansion and Development Pressure

A data center proposal should be assessed for more than its first phase.

The public should ask whether the site, infrastructure, zoning, land assembly, utility upgrades, or road design make future expansion likely. A project may begin as one building but create the conditions for a larger campus, additional data centers, industrial clustering, or speculative land development.

Communities should be especially cautious when infrastructure is oversized, adjacent land is optioned or purchased, zoning is broad, or the applicant describes future phases without including them in the full impact assessment.

The question is not only what the developer promises today.

The question is what the approval makes possible tomorrow.

Compatibility With Municipal and Regional Plans

A data center should be tested against existing plans, not inserted around them.

Does the proposal fit the municipality's land-use plan, regional growth strategy, housing plan, agricultural protection policy, climate plan, watershed plan, transportation plan, emergency services plan, economic development strategy, and infrastructure capacity plan?

If a project requires exceptions, rezoning, special agreements, or plan amendments, the public should know why the existing plan is being changed and who benefits from the change.

A proposal should not be allowed to override long-term planning simply because it arrives with a large investment number.

Public plans are promises communities make to themselves. They should not be casually rewritten for private infrastructure.

Core Questions

Site Selection

Why was this site chosen?

What other sites were considered?

Were brownfield, already-industrial, underused commercial, or lower-impact sites assessed?

Was the site chosen because it is appropriate, or because it is cheap, available, politically convenient, or easier to approve?

Does the site require rezoning, plan amendments, variances, exemptions, or special agreements?

Who owns the land?

Has adjacent land been purchased, optioned, assembled, or reserved for future expansion?

Current Land Use

What is the current land use?

Is the site farmland, wetland, forest, grassland, residential edge, industrial land, commercial land, public land, Indigenous land, or open space?

What uses surround the site?

Are there homes nearby?

Are there farms nearby?

Are there schools, hospitals, care facilities, parks, trails, playgrounds, or public gathering places nearby?

Are there culturally significant, historically significant, archaeological, or sacred sites nearby?

Future Land Use

What future land uses are planned around the site?

Is the area expected to become residential, mixed-use, agricultural, industrial, recreational, conservation, or public-service land?

Could housing, schools, care homes, parks, hospitals, or public facilities eventually surround the data center?

Will the facility limit future municipal growth?

Will the facility make nearby land less suitable for housing, farming, recreation, conservation, or public use?

Will future residents be exposed to noise, light, emissions, traffic, or emergency risks that are not present at the time of approval?

Does the approval create a long-term land-use conflict that future councils and residents will inherit?

Farmland

Will farmland be removed from production?

What class or quality of farmland is affected?

Will the project fragment farm parcels or make nearby farms harder to operate?

Will it affect irrigation, drainage, soil health, livestock, access roads, field operations, dust, or water availability?

Will construction or traffic interfere with seeding, harvesting, grazing, or farm equipment movement?

Has an agricultural impact assessment been completed?

Can the project be located on already-disturbed or non-agricultural land instead?

Wetlands, Forests, Grasslands, and Natural Areas

Does the site include or affect wetlands, streams, ponds, forests, native grasslands, riparian zones, floodplains, or aquifer recharge areas?

Will drainage patterns change?

Will stormwater runoff increase?

Will vegetation be cleared?

Will natural areas be fragmented?

Will buffers be protected?

Will the project affect flood risk, groundwater recharge, water quality, or local cooling?

Has the full disturbance area been assessed, including roads, utilities, substations, fencing, lighting, and future phases?

Housing and Sensitive Uses

How close is the facility to existing homes?

How close could future homes be built?

What setbacks are required?

Are the setbacks based on real-world sound, light, emissions, safety, and emergency risks?

Are schools, daycares, hospitals, clinics, seniors' residences, care homes, shelters, playgrounds, parks, or community facilities nearby?

Will vulnerable populations be affected?

Will the site create risks or burdens for people who cannot easily relocate?

Wildlife and Habitat

Does the site overlap with wildlife corridors, migration routes, breeding areas, nesting habitat, pollinator habitat, amphibian movement routes, riparian corridors, or habitat connectivity zones?

Will fencing, lighting, roads, noise, water changes, or vegetation clearing disrupt animal movement?

Has seasonal wildlife use been assessed?

Has nighttime impact been assessed?

Has cumulative habitat fragmentation been assessed?

Will mitigation be legally enforceable and monitored over time?

Transportation and Access

What construction traffic will the project generate?

What operational traffic will continue after construction?

Can local roads, bridges, and intersections safely support heavy equipment, fuel deliveries, transformers, generators, cooling systems, and ongoing maintenance?

Will road upgrades be required?

Who will pay for those upgrades?

Will traffic affect school buses, farm equipment, emergency vehicles, local businesses, pedestrians, cyclists, or public transit?

Will emergency access be reliable in winter, wildfire, flood, storm, or evacuation conditions?

Security and Community Character

What fencing, lighting, gates, cameras, barriers, patrols, or access restrictions will be used?

Will the site change the visual character of the area?

Will it block views, trails, informal access, rural landscape, or open space?

Will lighting affect nearby homes, wildlife, farms, or night skies?

Will landscaping and screening be required?

Who maintains screening and buffers over time?

Future Expansion

Is this project part of a larger campus or phased development?

What is the maximum buildout possible under the approval?

Will future phases require new public hearings?

Is infrastructure being sized for future expansion?

Are surrounding parcels being assembled?

Will the project encourage additional data centers or industrial development nearby?

What cumulative land-use impacts could result if this project becomes the anchor for a larger corridor?

Red Flags

A land-use proposal deserves greater scrutiny when the public hears:

"The site is currently vacant."

"The project is located away from most residents."

"The land is already designated for future development."
"Future phases will be reviewed later."
"The project will have minimal land impact."
"The facility will be screened from view."
"The site is near existing infrastructure."
"No significant habitat was identified."
"The area is not currently used for housing."
"The project is compatible with industrial development."
"Traffic impacts will be temporary."
"The facility will not affect surrounding land uses."

Open land is not empty land. Farmland is not unused land. Future residential land is not disposable land. Habitat is not protected by being noticed only after it is gone.

What Communities Should Ask For

Before approval, communities should ask for:
A complete site selection report.
A comparison of alternative sites, including already-industrial and lower-impact locations.
A current land-use map.
A future land-use map.
A municipal and regional planning compatibility assessment.
A farmland impact assessment, if agricultural land is involved.
A wetland, forest, grassland, habitat, and wildlife corridor assessment.
A housing proximity and future growth assessment.
A sensitive-site map showing schools, hospitals, care facilities, parks, playgrounds, shelters, and community facilities.
A transportation and construction access assessment.
A road and bridge capacity assessment.
A visual, lighting, fencing, and community character assessment.
A full buildout and future expansion plan.
A cumulative land-use impact assessment.
A public infrastructure cost assessment connected to land-use changes.
A clear explanation of any rezoning, variances, exemptions, or plan amendments required.
Legally enforceable setbacks, buffers, screening, lighting limits, habitat protections, road conditions, and expansion limits.

The Public Interest Standard

No data center should be approved until the public knows whether the site is appropriate for industrial-scale digital infrastructure, not only today, but for the life of the facility.

A proposal should be judged against farmland, wetlands, forests, housing, schools, hospitals, wildlife corridors, transportation routes, municipal growth, emergency access, and future community development.

A data center should not be allowed to solve a private siting problem by creating a public land-use conflict.

The land around a facility will not remain frozen in time. Communities grow. Open space fills in. Roads change. Homes move closer. Schools are built. Farms adapt. Wildlife routes narrow. Industrial clusters expand.

Land-use approval is not just permission to build.

It is a decision about what kind of future a place is being asked to accept.

8 - Sound, Vibration, and Light

A data center may look quiet from the road.

That does not mean it is quiet to live near.

Data centers can produce continuous sound from cooling systems, fans, chillers, pumps, transformers, electrical equipment, backup generators, truck traffic, construction activity, and maintenance operations. They may also produce vibration, low-frequency noise, tonal noise, pulsing sound, mechanical hum, and nighttime disturbance. They may operate twenty-four hours a day, seven days a week, in all seasons, during heat waves, during grid stress, and during emergency events.

The public should not ask only whether a data center meets a legal sound limit.

The better question is whether the sound, vibration, and light produced by the facility are fully understood, measured across the right frequencies, monitored at the right locations, reported in real time, and controlled in ways that protect people, livestock, wildlife, sleep, health, and community life.

Sound is not only a number.

It is a lived condition.

A facility that complies with a technical standard may still create a constant nighttime hum, low-frequency pressure, vibration, sleep disruption, livestock stress, wildlife disturbance, or a sense that quiet has been permanently taken from a place.

The Problem With Average Sound

Sound reports often rely on averages.

Averages can be useful, but they can also hide what people actually experience. A short loud event can disappear inside a long averaging period. A nighttime hum can be treated as acceptable because it does not exceed a daytime limit. A low-frequency vibration may be felt more than heard. A tonal sound may be more disturbing than a broad, neutral sound at the same decibel level. A backup generator test may be described as temporary even if it occurs regularly. Construction noise may be dismissed as short-term even if construction lasts for years across multiple phases.

The public should ask how sound is being measured, where it is being measured, when it is being measured, what frequencies are included, and whether the measurement reflects real-world conditions.

A single decibel figure is not enough.

Communities should ask for full-spectrum sound analysis, including low-frequency noise, tonal noise, impulsive noise, vibration, nighttime conditions, seasonal operations, backup generator testing, emergency operation, construction activity, and cumulative sound from all equipment and phases.

All Frequencies Matter

Not all sound is experienced the same way.

High-frequency sound may be sharp or piercing. Mid-frequency sound may be heard as ordinary mechanical noise. Low-frequency sound may travel farther, penetrate buildings more easily, pass through walls and windows, and be felt as pressure, rumble, vibration, or unease. Infrasound may be below the range many people consciously hear, but low-frequency energy can still contribute to disturbance depending on intensity, duration, building conditions, and individual sensitivity.

For this reason, data center sound assessments should not be limited to broad A-weighted decibel measurements alone.

A-weighted measurements can understate low-frequency sound because they are designed to approximate human hearing sensitivity, not necessarily the full range of disturbance experienced by people, animals, or structures. Communities should ask for sound data using multiple metrics where appropriate, including A-weighted, C-weighted, Z-weighted, octave-band, one-third-octave-band, tonal, low-frequency, and vibration measurements.

The goal is not to bury the public in technical language.

The goal is to prevent technical language from burying the impact.

If a facility produces sound across multiple frequencies, the public should be able to see those frequencies measured, reported, and regulated.

Measurement Points Matter

Where sound is measured can determine whether a problem is visible.

A proposal may measure sound at the property line. That may be useful, but it is not enough. People do not sleep at the property line. Livestock do not necessarily graze at the property line. Wildlife corridors, wetlands, barns, schools, homes, care facilities, and future development areas may sit beyond it.

Sound should be measured at multiple points, including:

Existing homes.

Future residential areas.

Schools, daycares, hospitals, clinics, care homes, shelters, and other sensitive sites.

Farmyards, barns, livestock areas, grazing areas, and animal shelters.

Wildlife corridors, wetlands, forests, nesting areas, breeding areas, and habitat edges.

Public trails, parks, campgrounds, and recreation areas.

The property line.

The nearest point of public access.

Areas where sound may reflect, channel, amplify, or accumulate because of topography, buildings, water, valleys, wind patterns, or atmospheric conditions.

Sound should also be measured at specific distances from the facility, not only at sensitive receptors. A distance-based measurement grid can help show how sound changes as it moves outward from the site.

The public should ask whether sound has been measured or modelled at regular distance intervals, such as 250 metres, 500 metres, 1 kilometre, 2 kilometres, and beyond where appropriate.

In rural or open landscapes, low-frequency sound, tonal hum, and nighttime noise may travel farther than residents expect. In valleys, near water, across open fields, or under certain weather conditions, sound may carry, reflect, or concentrate in ways that a simple property-line measurement will not reveal.

Distance-based measurements should not replace measurements at homes, farms, schools, care facilities, wetlands, wildlife corridors, or other sensitive locations. They should supplement them.

The public should also ask whether sound models account for real local conditions, including wind direction, temperature inversions, snow cover, vegetation loss, terrain, building reflections, and seasonal changes.

A sound model that assumes ideal conditions may not protect people living in real ones.

Nighttime Sound Is Different

Night changes sound.

At night, background noise often drops. People are trying to sleep. Windows may be open during warm seasons. Low-frequency sound may become more noticeable. Mechanical hum that is masked during the day may become dominant. Wildlife behaviour may change. Livestock may rest, breed, feed, or respond differently. Emergency generator tests, cooling surges, tonal sounds, and truck movements may be more disruptive after dark than during ordinary daytime activity.

For this reason, data center noise should be assessed separately for day, evening, night, weekends, holidays, heat waves, peak-load events, and emergency operation.

A facility should not be judged acceptable only because its average sound level over a long period appears low.

Sleep disruption is not averaged away.

Continuous Operation and Cumulative Sound

Data centers often operate continuously.

A sound that might be tolerable for an hour may become harmful or exhausting when it continues every day and every night. Constant sound can change the character of a home, farm, rural landscape, or natural area. It can reduce outdoor enjoyment, affect sleep, increase stress, interfere with communication, disturb animals, and make quiet places feel industrialized.

The public should ask not only how loud the facility will be, but how long the sound will continue.

Will fans run constantly?

Will cooling systems ramp up during hot weather?

Will transformers hum continuously?

Will backup generators be tested weekly or monthly?

Will construction occur in phases for years?

Will future buildings add more sound?

Will nearby substations, transmission lines, battery systems, roads, and other infrastructure contribute additional sound?

Cumulative sound should include all existing, proposed, and reasonably foreseeable sources, not only the first building in the application.

Backup Generators and Testing

Backup generators are often described as emergency equipment.

But emergency equipment may still be tested regularly. Generator testing can produce loud sound, low-frequency vibration, exhaust, odour, and traffic. If a facility has dozens or hundreds of generators, even scheduled testing can become a recurring burden.

The public should ask how many generators will be installed, what size they are, how often they will be tested, how long tests will last, whether testing will occur during the day or night, whether testing may happen simultaneously, and whether generator noise is included in the sound model.

Communities should also ask what happens during a real outage, grid emergency, wildfire, storm, or heat wave. A backup system that rarely operates in normal conditions may become a major sound and emissions source during exactly the moments when residents are already under stress.

Construction Noise and Vibration

Construction impacts should not be dismissed as temporary without examining the timeline.

Large data center projects may involve grading, blasting, pile driving, excavation, concrete work, steel erection, road building, substation construction, trenching, transmission upgrades, heavy truck traffic, backup-generator installation, and repeated phases of expansion. What is called temporary may last months or years.

Construction can produce noise, vibration, dust, traffic, lighting, and disruption to homes, farms, schools, wildlife, and local businesses. Vibration may affect buildings, wells, barns, sensitive equipment, livestock, nesting birds, aquatic habitat, or unstable soils.

The public should ask for a construction noise and vibration plan before approval, not after complaints begin.

Light Pollution and Night Operations

Sound is not the only nighttime impact.

Data centers may require security lighting, parking lighting, road lighting, loading-area lighting, construction lighting, emergency lighting, exterior building lighting, and lighting around substations, generators, fencing, gates, and cameras.

Poorly designed lighting can affect nearby homes, sleep, night skies, wildlife movement, birds, insects, bats, amphibians, livestock, and the rural or natural character of a place. It can also create glare, trespass onto neighbouring properties, alter views, and make an area feel less safe or less peaceful.

The public should ask whether lighting will be shielded, downward-facing, motion-controlled, spectrum-limited, dimmed during low-activity periods, and designed to protect dark skies and wildlife.

Security should not become an excuse for permanent light trespass.

Homes, Health, and Sleep

People experience sound and light inside their lives, not inside technical reports.

A data center near homes may affect sleep, concentration, outdoor use, mental stress, property enjoyment, and daily routines. People who work shifts, children, seniors, people with disabilities, people with sensory sensitivities, people with tinnitus, people with chronic illness, and people who cannot easily relocate may be more affected.

The public should ask whether the proposal protects real residents under real conditions.

Will sound be measured inside homes if complaints occur?

Will nighttime limits be stricter than daytime limits?

Will low-frequency noise be addressed?

Will tonal penalties apply?

Will lights be prevented from entering bedrooms?

Will complaints trigger independent investigation?

Will mitigation be required if people are affected even when the facility claims compliance?

A community should not be told that residents are imagining harm because the wrong metric was used to measure it.

Livestock, Wildlife, and Ecosystems

Sound, vibration, and light can affect more than people.

Livestock may respond to continuous noise, sudden noise, vibration, light changes, traffic, generator testing, and construction disturbance. Wildlife may alter movement, feeding, breeding, nesting, migration, predator avoidance, and habitat use because of sound and light. Birds, bats, insects, amphibians, fish, and mammals may all be affected in different ways.

The public should ask whether animal impacts have been assessed directly, not treated as an afterthought.

Has livestock behaviour been considered?

Have breeding and nesting seasons been considered?

Have nocturnal species been considered?

Have wetlands, riparian areas, forests, grasslands, and wildlife corridors been considered?

Will lighting and sound affect pollinators, migratory birds, amphibians, bats, or aquatic systems?

Will monitoring continue after the facility begins operation?

Noise and light are habitat changes.

Ongoing Measurement and Real-Time Reporting

Pre-approval modelling is not enough.

A sound study predicts what may happen. It does not prove what will happen. Once the facility is operating, the public should be able to compare actual conditions against the promises made during approval.

For that reason, data centers should be required to use ongoing sound, vibration, and light monitoring at multiple public-interest locations. Monitoring should include all relevant frequencies,

nighttime conditions, low-frequency sound, tonal sound, vibration, generator testing, emergency operation, construction phases, and cumulative impacts from future expansion.

Real-time reporting should be required where feasible.

The public should not have to rely only on company summaries, annual reports, or complaint forms. Residents should be able to see whether sound and light levels are within approved limits. Regulators should be able to identify exceedances quickly. Complaints should be compared against actual monitoring data, not dismissed because a model predicted compliance.

Monitoring data should be public, searchable, understandable, archived, and independently auditable.

If the facility exceeds limits, there should be automatic consequences, including investigation, public notice, mitigation, penalties, operating restrictions, or permit review.

Accountability should not depend on residents sacrificing sleep long enough to prove they are being disturbed.

Core Questions

Sound Modelling

What sound sources are included in the model?

Does the model include cooling systems, fans, chillers, pumps, transformers, substations, batteries, backup generators, truck traffic, maintenance, alarms, construction, and future phases?

Does the model include cumulative sound from nearby industry, roads, substations, transmission infrastructure, and other data centers?

Does the model assess daytime, evening, nighttime, weekend, seasonal, heat-wave, and emergency conditions separately?

Does the model account for wind direction, temperature inversions, snow cover, vegetation loss, terrain, water, building reflection, and atmospheric conditions?

Was the model prepared by an independent acoustic expert?

Will the model be peer reviewed?

Frequency Range and Metrics

What frequencies are being measured?

Are low-frequency noise and infrasound considered?

Are tonal sounds identified?

Are impulsive sounds identified?

Are vibration impacts assessed?

Are A-weighted measurements used?

Are C-weighted or Z-weighted measurements also used where needed?

Are octave-band or one-third-octave-band results provided?

Are maximum levels, minimum levels, averages, peaks, and duration reported separately?

Are nighttime sound limits stricter than daytime limits?

Measurement Points

Operations

Will the facility operate twenty-four hours a day?

Which equipment runs continuously?

Which equipment ramps up during hot weather or high workload?

Will cooling systems produce more noise during heat waves?

Will AI or high-density computing workloads increase cooling noise?

Will transformers, fans, pumps, chillers, and electrical systems produce tonal or low-frequency sound?

Can noisy operations be restricted at night?

Backup Generators

How many backup generators will be installed?

What size are they?

Where will they be located?

How often will they be tested?

How long will tests last?

Will tests occur during daytime only?

Can multiple generators be tested at once?

Will generator testing be publicly scheduled?

Will generator sound, vibration, and emissions be monitored in real time?

What happens during extended outages or grid emergencies?

Construction Noise and Vibration

How long will construction last?

Will construction occur in phases?

What equipment will be used?

Will pile driving, blasting, grading, excavation, trenching, concrete work, road construction, substation construction, or transmission work occur?

What vibration limits apply?

Will nearby wells, homes, barns, livestock facilities, sensitive equipment, wetlands, and wildlife habitat be protected?

Will construction hours be restricted?

Will residents receive notice before loud or vibration-heavy work?

Will construction noise and vibration be monitored continuously?

Light

What lighting will be installed?

Will lighting operate all night?

Will lighting be shielded and downward-facing?

Will lighting be motion-controlled?

Will lights be dimmed during low-activity periods?

What colour temperature will be used?

Will blue-rich light be avoided near homes and habitat?

Will light trespass onto neighbouring properties be prohibited?

Will glare be assessed from homes, roads, farms, trails, and public areas?

Will dark-sky standards be applied?

Will lighting impacts on birds, bats, insects, amphibians, livestock, and wildlife corridors be assessed?

Homes, Livestock, Wildlife, and Sensitive Sites

How close are homes and farms to the facility?

How close are schools, hospitals, care homes, shelters, parks, and playgrounds?

How close are barns, pastures, calving areas, poultry barns, riding facilities, kennels, or other animal facilities?

How close are wetlands, forests, riparian zones, grasslands, nesting areas, breeding areas, and wildlife corridors?

Have people with sleep sensitivity, tinnitus, sensory sensitivities, chronic illness, or limited ability to relocate been considered?

Have livestock and wildlife impacts been assessed by qualified experts?

Will post-construction monitoring include human, livestock, and wildlife impacts?

Ongoing Monitoring and Reporting

Will sound, vibration, and light be monitored after construction?

Will monitoring be continuous?

Will all relevant frequencies be measured?

Will low-frequency sound be separately reported?

Will generator testing be separately reported?

Will nighttime data be separately reported?

Will real-time data be publicly available?

Will data be archived?

Will the public be able to compare actual levels with approved limits?

Will monitoring be independently audited?

Who receives complaints?

How quickly must complaints be investigated?

What happens if limits are exceeded?

Can operations be reduced, equipment modified, generators rescheduled, lighting changed, or permits reopened?

Red Flags

A sound, vibration, or light proposal deserves greater scrutiny when the public hears:

"The facility will meet applicable noise standards."

"Noise impacts will be minimal."

"The nearest homes are far away."

"Sound will be measured at the property line."
"Backup generators are only for emergencies."
"Construction impacts will be temporary."
"Lighting is required for security."
"Low-frequency noise is not expected to be an issue."
"The model shows compliance."
"Future phases will be assessed later."
"Complaints will be handled through normal processes."
"Monitoring will occur if needed."

Compliance is not the same as comfort. Averages are not the same as sleep. Property lines are not the same as bedrooms. A model is not the same as lived experience.

What Communities Should Ask For

Before approval, communities should ask for:
A full acoustic impact assessment.
Full-spectrum sound analysis, including low-frequency noise.
A vibration assessment.
A nighttime noise assessment.
A tonal and impulsive noise assessment.
A construction noise and vibration plan.
A backup generator testing and emergency-operation noise plan.
A lighting impact assessment.
A dark-sky and wildlife-sensitive lighting plan.
A map of all measurement points.
A cumulative sound model including future phases and nearby infrastructure.
A human health and sleep impact assessment where homes or sensitive sites may be affected.
A livestock and wildlife disturbance assessment where farms, habitat, or corridors may be affected.
Legally enforceable sound, vibration, and lighting limits.
Continuous monitoring requirements.
Real-time public reporting where feasible.
Independent auditing of monitoring data.
A complaint-response system with deadlines, public reporting, and enforceable remedies.
Clear penalties, operating restrictions, and permit-review triggers if limits are exceeded.

The Public Interest Standard

No data center should be approved until the public understands the real sound, vibration, and light impacts of the facility under normal, nighttime, construction, heat-wave, backup-generator, emergency, and full-buildout conditions.

Sound must be measured across the frequencies people and animals may experience.

Monitoring must occur where impacts are felt, not only where they are convenient to measure.

Reporting must continue after approval, not end with a prediction.

A community should not be asked to trade quiet nights, healthy sleep, animal well-being, dark skies, or ecological stability for a facility whose impacts are hidden inside averages, models, or property-line measurements.

Quiet is not empty.

Darkness is not wasted.

Both are part of the public interest.

9 - Heat, Cooling, and Waste Heat

A data center produces heat because computation produces heat.

Every server, chip, rack, power supply, transformer, battery system, pump, fan, and cooling system is part of a larger thermal process. Electricity enters the facility. Computation happens. Heat is produced. That heat must go somewhere.

The public should not treat cooling as a minor technical detail.

Cooling determines water use, electricity demand, noise, equipment layout, emissions, chemical use, discharge, emergency planning, and the surrounding thermal footprint of the facility. It can affect nearby homes, workers, animals, plants, waterways, air temperature, microclimates, and local infrastructure. It can also determine whether a data center wastes a major energy byproduct or turns that heat into a public benefit.

The question is not only:

How will the facility cool itself?

The better question is:

Where does the heat go, who is affected by it, and could that heat be put to public use?

Heat Is Not Gone Because It Is Moved

Cooling does not eliminate heat.

It moves heat.

A data center may reject heat into the air through cooling towers, dry coolers, chillers, fans, rooftop units, side-mounted units, or mechanical yards. It may reject heat into water through liquid cooling, heat exchangers, discharge systems, or industrial water loops. It may store heat temporarily. It may vent heat into the surrounding environment. It may concentrate heat near equipment yards, rooflines, walls, roadways, loading areas, or utility zones.

A proposal should not be allowed to describe cooling as though heat simply disappears.

If the facility produces heat, the public should know how much heat is produced, where it is rejected, at what temperature, under what conditions, and how those conditions change during peak workload, heat waves, drought, grid stress, equipment failure, or full buildout.

Cooling Methods Matter

Different cooling systems create different impacts.

Air cooling may reduce direct water use but require more electricity, more fans, more equipment, and more noise. Evaporative cooling may reduce electricity demand but consume water and create discharge, chemical treatment needs, visible plumes, and drought concerns. Liquid cooling may improve efficiency for dense computing loads, including AI workloads, but may require specialized fluids, heat exchangers, maintenance systems, leak prevention, and waste handling. Hybrid systems may shift between modes depending on temperature, humidity, water availability, energy cost, and operational demand.

The public should not accept "efficient cooling," "closed-loop cooling," "low-water cooling," or "advanced cooling" without specific explanation.

The facility should disclose the cooling method, cooling equipment, expected heat load, water use, energy use, chemicals, discharge, noise, maintenance requirements, failure modes, and emergency cooling plan for each phase of the project.

Heat Island Effects

A large data center can contribute to localized heat.

The facility may replace fields, vegetation, wetlands, forests, or open soil with buildings, roads, roofs, concrete, asphalt, gravel, substations, fencing, parking, and mechanical equipment. These surfaces can absorb and retain heat. Cooling equipment may reject warm air into the local environment. Backup generators, transformers, and electrical systems may add further heat. Reduced vegetation can decrease shading and natural cooling.

This can contribute to a local heat island effect.

A heat island may affect nearby homes, workers, livestock, wildlife, plants, insects, soil moisture, stormwater temperature, energy demand, and public comfort. It may be especially important during heat waves, drought, wildfire smoke events, and periods when vulnerable people are already at risk.

The public should ask whether the project has assessed its thermal footprint, not only its building footprint.

Will the facility raise local air temperatures?

Will it increase nighttime heat retention?

Will waste heat be concentrated near neighbouring properties?

Will hot exhaust affect public roads, trails, farms, homes, or habitat?

Will vegetation removal reduce natural cooling?

Will roofs, paving, and equipment yards increase reflected or stored heat?

Will the project worsen heat stress for people, animals, plants, or ecosystems nearby?

A data center should not be evaluated only by whether its servers stay cool. The surrounding community matters too.

Waste Heat: Burden or Public Benefit?

A data center produces a continuous stream of heat.

In many cases, that heat is treated as waste. It is vented into the air, rejected through cooling systems, discharged into water, or otherwise removed from the facility as a problem to be managed. But heat is also energy. Depending on temperature, technology, proximity, infrastructure, and economics, waste heat may be recoverable and useful.

The public should ask whether waste heat recovery has been assessed.

Could the heat be used for district heating?

Could it heat public buildings?

Could it support schools, hospitals, recreation centres, libraries, municipal buildings, seniors' homes, social housing, or emergency shelters?

Could it heat greenhouses, food production facilities, aquaculture systems, industrial processes, or community facilities?

Could it reduce public heating bills, local emissions, or fuel use?

Could waste heat recovery be built into the project from the beginning, rather than considered later when infrastructure is harder and more expensive to add?

A data center should not be allowed to impose its heat burden on a community while wasting a potential public benefit.

Not every site will be suitable for waste heat reuse. Temperature levels, distance, seasonality, infrastructure cost, ownership, and reliability all matter. But the public has the right to know whether reuse was studied seriously, what options were considered, why they were accepted or rejected, and whether the project design preserves the possibility of future heat recovery.

If a facility receives public subsidies, tax incentives, discounted power, public land, water rights, or infrastructure support, then waste heat should be treated as part of the public-interest bargain.

District Heating and Community Energy

District heating systems move heat from a source to multiple buildings through a shared thermal network. In some places, data center waste heat can be integrated into district energy systems, especially where there are nearby public buildings, dense residential areas, greenhouses, universities, hospitals, industrial users, or municipal facilities.

The public should ask whether the data center site was selected or designed with district heating potential in mind.

A facility located far from usable heat customers may make waste heat recovery difficult. A facility built near public buildings, housing, greenhouses, or industrial users may create opportunities. But those opportunities may be lost if heat recovery infrastructure, connection points, easements, temperature levels, or ownership agreements are not considered before construction.

Communities should ask whether the project includes:

A waste heat recovery feasibility study.

Thermal mapping of nearby heat users.

Connection points for future district energy.

A plan for public or community use of recovered heat.

Agreements on pricing, ownership, maintenance, and reliability.

A requirement that waste heat not be privatized after public infrastructure makes recovery possible.

The goal is not to force every project into a district heating model.

The goal is to prevent useful heat from being wasted because nobody asked the question early enough.

Thermal Pollution and Water Impacts

If heat is transferred to water, the public should ask where that warmed water goes.

Thermal pollution can affect rivers, lakes, wetlands, stormwater systems, groundwater, aquatic species, algae growth, dissolved oxygen, fish habitat, amphibians, invertebrates, and downstream

users. Even treated discharge may create ecological stress if it changes temperature in sensitive environments, especially during low-flow periods, drought, or summer heat.

A facility should disclose whether water will leave the site warmer than it entered.

If heated discharge is possible, the proposal should identify discharge temperature, volume, timing, receiving environment, seasonal variation, low-flow conditions, cumulative impacts, monitoring methods, and enforcement limits.

The public should not be told that discharge is safe only because it meets a general permit standard. The receiving environment matters.

A small stream, wetland, shallow aquifer, stormwater pond, or already stressed river may respond differently than a large, fast-moving water body. Seasonal timing matters. Drought matters. Existing thermal stress matters. Aquatic life matters.

Emergency Cooling and Failure Scenarios

Cooling failure is not only a business risk.

It can become a public risk.

If cooling systems fail, servers can overheat. Backup systems may activate. Generators may run. Emergency water may be needed. Fire risk may increase. Fans, pumps, alarms, and emergency equipment may operate differently. Fuel deliveries may increase. Traffic may rise. Noise and emissions may spike. If a facility contains battery systems, specialized coolants, fuel storage, or other industrial equipment, emergency cooling failures may create additional hazards.

The public should ask what happens when the cooling plan does not work as designed.

What happens during a heat wave?

What happens during drought?

What happens during a power outage?

What happens if water restrictions are in place?

What happens if pumps fail?

What happens if a cooling tower, chiller, heat exchanger, liquid cooling loop, or control system fails?

What happens if wildfire smoke, flooding, freezing rain, extreme cold, or storms affect the cooling system?

What happens if the facility expands but cooling infrastructure does not perform as expected?

Emergency cooling plans should be public enough for communities and emergency responders to understand the risks, while still protecting legitimate security details.

Climate Change and Future Conditions

A cooling system designed for past climate conditions may not be adequate for the future.

Heat waves are becoming more severe in many regions. Drought can reduce water availability. Wildfire smoke can affect air handling systems. Extreme storms can affect power supply. Warmer nights can reduce the effectiveness of certain cooling methods. Higher humidity can change cooling performance. Grid stress can coincide with peak cooling demand.

A data center expected to operate for decades should be assessed under future climate scenarios, not only historical weather data.

The public should ask whether the cooling system has been tested against higher temperatures, longer heat waves, drought, reduced water availability, grid constraints, wildfire smoke, and full-buildout operations.

A facility should not be approved based on a climate that no longer exists.

Cumulative Thermal Burden

One facility may have a manageable heat impact.

Several facilities may not.

A data center campus, industrial corridor, or cluster of facilities can create cumulative heat effects through multiple buildings, large paved surfaces, repeated heat rejection, transmission infrastructure, substations, backup systems, road networks, and reduced vegetation.

The public should ask whether the thermal assessment includes only the first building, the full buildout, or the cumulative impact of other existing and reasonably foreseeable developments.

Heat should be assessed at the scale people and ecosystems experience it, not only at the scale the application prefers.

Core Questions

Heat Production

How much heat will the facility produce during normal operation?

How much heat will it produce at peak workload?

How much heat will it produce during heat waves?

How much heat will it produce at full buildout?

How does heat production vary by season, tenant, workload, and AI or high-density computing use?

Where will heat be rejected?

At what temperature will heat be rejected?

Will heat be released into air, water, ground systems, buildings, or another medium?

Cooling Method

What cooling method will be used?

Will the facility use air cooling?

Will it use evaporative cooling?

Will it use liquid cooling?

Will it use immersion cooling?

Will it use hybrid cooling?

Will it use chillers, cooling towers, dry coolers, pumps, fans, heat exchangers, or rooftop units?

How much electricity does the cooling system require?

How much water does it require?

What chemicals, coolants, or treatment systems does it require?

How loud is the cooling equipment under normal, peak, nighttime, and heat-wave conditions?

Can the cooling method change later without public review?

Heat Island Effects

Will the project increase local air temperatures?

Has a heat island assessment been completed?

Will roofs, walls, asphalt, concrete, gravel, substations, roads, and equipment yards increase heat absorption or retention?

How much vegetation will be removed?

Will tree canopy, wetlands, grasslands, or natural cooling areas be lost?

Will the facility increase nighttime heat retention?

Will nearby homes, farms, livestock, schools, care homes, workers, parks, trails, or wildlife habitat be affected?

What heat mitigation measures will be required?

Will the site use reflective roofing, green buffers, tree canopy, permeable surfaces, shaded parking, reduced paving, or other cooling design?

Who maintains heat mitigation measures over time?

Waste Heat Recovery

Will waste heat be captured or reused?

Has a waste heat recovery feasibility study been completed?

Could waste heat be used for district heating?

Could it heat public buildings?

Could it support schools, hospitals, libraries, recreation centres, municipal buildings, seniors' homes, shelters, or social housing?

Could it heat greenhouses, aquaculture systems, food production, industrial processes, or community facilities?

What temperature is the waste heat?

Is the temperature high enough for practical reuse?

What infrastructure would be required?

Who would pay for heat recovery infrastructure?

Who would own and operate it?

Would recovered heat be offered at a public-benefit rate?

If waste heat recovery is rejected, why?

Will the facility be built with connection points so heat recovery remains possible later?

District Energy

Are there nearby buildings or facilities that need heat?

Has a thermal map been prepared?

Could the data center connect to an existing or future district heating system?

Could the site be moved or redesigned to improve heat reuse potential?

Would public infrastructure be needed?

Would public buildings receive priority access to recovered heat?

Could recovered heat reduce municipal energy costs or emissions?

Are long-term agreements proposed to guarantee public access to recovered heat?

Thermal Pollution and Discharge

Will heated water be discharged?

Where will heated water go?

What will the discharge temperature be?

How will discharge temperature vary by season, workload, and weather?

Will discharge enter a river, lake, wetland, stormwater system, sewer system, groundwater system, or treatment facility?

Has the receiving environment been assessed for thermal sensitivity?

Have low-flow, drought, and summer heat conditions been assessed?

Could discharge affect fish, amphibians, aquatic insects, algae growth, dissolved oxygen, wetlands, or downstream users?

Will discharge temperature be monitored in real time?

Will monitoring results be public?

Equipment Failure and Emergency Cooling

What happens if the cooling system fails?

What backup cooling systems exist?

Will emergency cooling require extra water?

Will emergency cooling require backup generators?

Will emergency cooling increase noise, emissions, traffic, or discharge?

What happens during a heat wave?

What happens during drought?

What happens during grid failure?

What happens during wildfire smoke, flooding, storms, or extreme cold?

How long can the facility operate safely without normal cooling?

What emergency response agencies have reviewed the cooling failure plan?

Will the public be notified during cooling-related emergencies?

Future Climate and Full Buildout

Was the cooling system assessed under future climate scenarios?

Were higher temperatures, longer heat waves, drought, wildfire smoke, and grid stress included?

Was full buildout assessed?

Can later phases increase heat rejection without new review?

Will surrounding development reduce airflow or worsen heat accumulation?

Will future residential, agricultural, public, or ecological uses be affected by the facility's long-term thermal footprint?

Monitoring and Accountability

Will heat rejection be monitored after construction?

Will local temperature impacts be monitored?
Will water discharge temperature be monitored?
Will cooling system performance be publicly reported?
Will waste heat recovery performance be publicly reported if implemented?
Will complaints about heat, humidity, plumes, or thermal impacts trigger investigation?
Who verifies the data?
What penalties apply if thermal limits are exceeded?
Can permits be reviewed if cooling impacts are greater than predicted?

Red Flags

A heat, cooling, or waste heat proposal deserves greater scrutiny when the public hears:
"Cooling impacts will be minimal."
"The facility will use advanced cooling."
"The system is closed loop."
"Waste heat recovery may be considered later."
"The project will not affect local temperatures."
"Cooling details will be finalized after approval."
"Heat will be managed on site."
"No significant discharge impacts are expected."
"The facility will use efficient equipment."
"Emergency cooling is unlikely to be needed."
"The project is designed for future climate conditions."
"District heating is not feasible."

Cooling does not eliminate heat. It moves it.
Waste heat is not harmless because it is inconvenient.
A heat island is not avoided because it was not measured.
Future reuse is not protected unless the design makes room for it.

What Communities Should Ask For

Before approval, communities should ask for:
A full heat production and heat rejection assessment.
A cooling system description in plain language.
A comparison of cooling alternatives.
A water and energy analysis for each cooling option.
A heat island assessment.
A thermal impact assessment for nearby homes, farms, public facilities, workers, livestock, wildlife, plants, and ecosystems.
A thermal discharge assessment, if water discharge is possible.
A future climate cooling assessment.
A full-buildout cooling assessment.
An emergency cooling and equipment failure plan.

A waste heat recovery feasibility study.

A district energy opportunity assessment.

A map of potential public, community, agricultural, greenhouse, industrial, and residential heat users.

A plan for preserving future waste heat recovery options if immediate reuse is not feasible.

A public reporting plan for heat rejection, cooling performance, discharge temperature, and emergency cooling events.

Legally enforceable limits on heat discharge, thermal pollution, cooling changes, and emergency operation.

Clear penalties, mitigation requirements, and permit-review triggers if thermal impacts exceed predictions.

The Public Interest Standard

No data center should be approved until the public understands how much heat it will produce, how that heat will be managed, whether cooling will burden water or electricity systems, whether local heat island effects have been assessed, and whether waste heat can be put to public use.

A community should not be asked to accept heat as a private byproduct while receiving none of its possible public benefit.

If a facility produces heat continuously, then the public has the right to ask whether that heat will warm public buildings, greenhouses, homes, schools, hospitals, or community facilities — or whether it will simply be dumped into the air, water, and surrounding environment.

Cooling is not the end of the heat question.

It is where the heat question begins.

10 - Air, Emissions, and Backup Systems

A data center may be marketed as clean infrastructure.

That does not mean it has no emissions.

Even when a facility claims to run on renewable electricity, it may still rely on diesel generators, gas turbines, fuel storage, battery systems, fire suppression chemicals, cooling chemicals, transformers, emergency systems, construction equipment, maintenance vehicles, and truck traffic. These systems can affect local air quality, greenhouse gas emissions, fire risk, chemical exposure, emergency planning, and public health.

The public should not ask only whether a data center is "green."

The better question is:

What does the facility emit, under what conditions, how often, who is exposed, who measures it, and what happens when something goes wrong?

Air impacts are not limited to normal operations. They may occur during construction, generator testing, grid outages, heat waves, wildfire events, equipment failure, emergency operation, fuel deliveries, battery incidents, fire suppression releases, maintenance, and full-buildout expansion.

A data center's clean-energy claim should never be allowed to erase its local air and backup-system footprint.

Backup Power Is Not a Footnote

Data centers are built to avoid downtime.

That means backup systems are central to their operation. A facility may include rows of diesel generators, gas turbines, fuel tanks, battery energy storage systems, uninterruptible power supplies, switchgear, transformers, cooling backup, fire suppression systems, and emergency controls.

These systems may be described as rarely used, but rare use is not the same as no impact.

Backup generators may be tested regularly. Fuel must be stored and delivered. Batteries must be cooled, maintained, replaced, and protected from fire. Fire suppression systems may involve chemicals or gases. Emergency systems may operate during outages, grid stress, storms, wildfire, heat waves, or equipment failure.

The public should know what backup systems are being installed before approval is granted.

A facility should not be allowed to present itself as a low-impact building while hiding a private power plant, fuel depot, battery installation, or chemical fire-suppression system inside the technical appendices.

Diesel Generators and Gas Turbines

Many data centers rely on diesel generators or gas turbines for backup power.

These systems can emit nitrogen oxides, sulfur dioxide, carbon monoxide, particulate matter, volatile organic compounds, greenhouse gases, and other pollutants depending on the fuel, engine type, pollution controls, maintenance, testing schedule, and operating conditions.

The public should ask how many generators or turbines will be installed, how large they are, where they are located, what fuel they use, how often they will run, how often they will be tested, and what emissions they will produce.

A single small backup generator may be one thing.

Dozens or hundreds of large generators across a data center campus are another.

Even if each unit is permitted separately, the public should understand the cumulative emissions of the full facility.

Testing Schedules Matter

Backup systems are often tested.

Testing may occur weekly, monthly, quarterly, annually, or after maintenance. It may involve one generator at a time or multiple units. It may occur under no-load or full-load conditions. It may last minutes or hours. It may happen during the day, evening, weekend, or in some cases during periods when residents are home, animals are nearby, or local air quality is already poor.

The public should ask for a clear testing schedule before approval.

Testing emissions should be included in air quality modelling. Testing noise should be included in acoustic modelling. Testing fuel use should be included in greenhouse gas estimates. Testing schedules should be public, and testing should be restricted during poor air quality events, high heat, wildfire smoke, school hours near sensitive sites, or other conditions where impacts may be greater.

Backup generator testing is not an emergency.

It is a planned activity, and planned activities can be regulated.

Emergency Operation and Grid Stress

A backup system may run rarely — until it does not.

Extreme weather, wildfires, storms, heat waves, grid failures, transmission constraints, equipment failures, cyberattacks, and demand emergencies can all cause backup systems to operate. During those periods, surrounding communities may already be under stress. Air quality may already be poor. Emergency services may already be stretched. Residents may already be coping with heat, smoke, evacuation risk, power loss, or health concerns.

The public should ask what happens when the facility enters emergency mode.

How long can generators run?

How much fuel is stored on site?

How often will fuel deliveries be needed?

What emissions occur during extended operation?

Could generators run during wildfire smoke events?

Could they run during heat waves when ozone or particulate matter is already a concern?

Could a data center continue operating on backup power while nearby residents experience outages?

Will emergency operation trigger public notice, monitoring, or reporting?

Emergency planning should not focus only on keeping the servers online. It should also protect the surrounding community.

Particulate Emissions and Local Air Quality

Air quality is local.

A facility's emissions may be small in a regional inventory but significant for nearby residents, workers, farms, schools, care homes, or communities already exposed to other sources of pollution. Local air impacts can depend on wind, terrain, temperature inversions, building layout, stack height, generator placement, traffic routes, and existing background pollution.

The public should ask whether air modelling reflects real local conditions.

Averages may hide short-term exposure. Annual totals may hide peak events. Regional climate claims may hide neighbourhood-level air quality impacts. A facility that meets a broad emissions standard may still create local burdens if emissions concentrate near homes, barns, schools, hospitals, daycares, seniors' residences, or low-lying areas where air can pool.

Air quality assessment should include normal operations, generator testing, emergency operation, construction emissions, traffic, fuel deliveries, full buildout, and cumulative impacts from nearby industry or other data centers.

Greenhouse Gas Emissions

A data center's climate impact cannot be measured only at the building wall.

Greenhouse gas emissions may come from grid electricity, backup generators, gas turbines, fuel deliveries, construction materials, concrete, steel, refrigerants, cooling systems, battery manufacturing, equipment replacement, and new power generation built to serve the facility.

A project may claim carbon neutrality through offsets, renewable energy certificates, or annual energy matching while still causing real emissions during peak demand, backup operation, construction, or supply-chain activity.

The public should ask for a full greenhouse gas assessment that separates direct emissions, electricity-related emissions, construction emissions, backup-system emissions, refrigerant leakage, and embodied emissions where possible.

A climate claim should be measurable, enforceable, and understandable.

Batteries and Fire Risk

Battery systems may reduce diesel generator use, support grid stability, or provide short-term backup power. They may also introduce fire, smoke, chemical, thermal runaway, explosion, water use, toxic gas, runoff, and waste-management concerns depending on the battery chemistry, size, design, location, and emergency response plan.

The public should not treat battery storage as automatically clean or harmless.

Battery systems should be assessed for fire risk, cooling needs, emergency access, separation distances, fire suppression methods, toxic emissions, water runoff, replacement cycles, recycling, and end-of-life disposal.

The public should also ask whether local fire departments have the training, equipment, staffing, water supply, protective gear, and response plans needed for a battery incident.

A battery system that protects a data center from downtime should not leave the surrounding community unprepared for the risks it creates.

Fire Suppression Chemicals and Emergency Releases

Data centers require fire protection.

Depending on the facility design, fire suppression may involve water, clean agents, inert gases, foam, chemical systems, specialized suppression for battery rooms, transformer fire protection, or other systems. Some fire suppression systems can create chemical exposure, oxygen-displacement risks, runoff concerns, or environmental consequences if released.

The public should ask what fire suppression systems will be used, what substances they contain, where they are stored, how releases are prevented, what happens if they are discharged, and how workers, first responders, residents, animals, waterways, and stormwater systems will be protected.

Fire suppression should be part of environmental review, not only building-code compliance.

Refrigerants, Coolants, and Chemical Systems

Cooling systems may involve refrigerants, coolants, corrosion inhibitors, biocides, anti-scaling agents, cleaning chemicals, water-treatment chemicals, dielectric fluids, or other substances.

Some refrigerants have high global warming potential if leaked. Some coolants and treatment chemicals may require special handling, storage, disposal, and spill response. Some systems may be low-risk under ordinary conditions but create concerns during leaks, fires, maintenance failures, or emergency response.

The public should ask for a chemical inventory and a plain-language explanation of how chemicals will be stored, monitored, used, replaced, discharged, and disposed of.

A facility should not receive approval before the public knows what substances will be on site.

Construction Emissions

Air impacts begin before the servers are installed.

Construction may involve diesel equipment, trucks, excavation, grading, concrete work, asphalt, generators, welding, dust, road building, transmission construction, substation construction, and material delivery. If the project is large or phased, construction emissions may continue for years.

The public should ask for a construction emissions and dust-control plan.

That plan should include diesel equipment standards, idling restrictions, haul routes, dust suppression, concrete and asphalt impacts, construction generator use, nearby sensitive sites, school and hospital routes, farm impacts, worker exposure, and public reporting.

Temporary construction impacts are still impacts, especially when temporary means multi-year.

Cumulative Emissions

A data center should not be assessed as though it exists alone if it does not.

Cumulative emissions may come from nearby industry, highways, rail lines, airports, power plants, substations, transmission corridors, warehouses, construction sites, backup generators, additional data centers, and future phases of the same campus.

If multiple facilities are proposed in the same region, each project may appear manageable on its own while the combined air burden becomes significant.

The public should ask whether cumulative air quality, greenhouse gas, backup power, and emergency emissions have been assessed at full buildout.

Monitoring and Real-Time Reporting

Pre-approval modelling is not enough.

Air quality impacts should be monitored after construction, especially if the facility uses diesel generators, gas turbines, battery systems, fuel storage, chemical fire suppression, or other systems that can create local impacts during testing or emergencies.

The public should ask for ongoing monitoring of generator operation, emissions, fuel use, air quality, particulate matter, nitrogen oxides, greenhouse gases, battery incidents, fire suppression releases, and emergency events where appropriate.

Real-time or near-real-time reporting should be required for generator testing, emergency operation, exceedances, incidents, and complaints.

The public should not have to discover after the fact that generators ran for hours, fuel was spilled, smoke was released, a battery incident occurred, or air quality limits were exceeded.

Core Questions

Backup Systems

What backup power systems will be installed?
Will the facility use diesel generators?
Will it use gas turbines?
Will it use battery storage?
Will it use fuel cells?
Will it use uninterruptible power supplies?
Will it use other emergency systems?
How many units will be installed?
What is the size and capacity of each unit?
Where will backup systems be located?
Are backup systems sized for the first phase or full buildout?
Can additional backup systems be added later without public review?

Diesel Generators and Gas Turbines

How many diesel generators or gas turbines will be installed?
What fuel will they use?
How much fuel will be stored on site?
Where will fuel be stored?
How often will fuel be delivered?
What spill prevention systems will be used?
What pollution controls will be installed?
What emissions will occur during testing?
What emissions will occur during emergency operation?

How long can the facility run on backup power?

Will generator stacks be located away from homes, schools, farms, hospitals, care facilities, and public spaces?

Testing Schedules

How often will backup generators be tested?

How long will each test last?

Will testing occur under load?

Will multiple generators be tested at the same time?

Will testing be restricted to daytime hours?

Will testing be prohibited during poor air quality events, wildfire smoke, heat waves, school hours near sensitive sites, or other vulnerable periods?

Will testing schedules be made public?

Will actual testing events be reported publicly?

Will emissions and noise during testing be monitored?

Air Quality

What pollutants will be emitted?

Will the assessment include particulate matter, nitrogen oxides, sulfur dioxide, carbon monoxide, volatile organic compounds, hazardous air pollutants, greenhouse gases, and any other relevant emissions?

What are the existing background air quality conditions?

Are nearby communities already exposed to industrial, traffic, agricultural, wildfire, or other pollution sources?

Will modelling include temperature inversions, wind patterns, terrain, stack height, building downwash, seasonal conditions, and worst-case scenarios?

Will short-term peak exposures be assessed separately from annual averages?

Will homes, schools, hospitals, care facilities, farms, barns, playgrounds, parks, and workplaces be included as sensitive receptors?

Greenhouse Gases

What are the direct greenhouse gas emissions from the facility?

What emissions come from grid electricity?

What emissions come from backup generators or gas turbines?

What emissions come from refrigerants or coolant leaks?

What emissions come from construction materials, concrete, steel, equipment, and batteries?

What emissions come from new generation or grid upgrades required by the project?

Are climate claims based on actual emissions reductions, offsets, renewable energy certificates, or accounting methods?

Are greenhouse gas claims enforceable?

Will actual emissions be publicly reported?

Battery Systems

Will battery storage be used?
What type of batteries will be installed?
What is the storage capacity?
Where will batteries be located?
What fire risks exist?
What toxic gases, smoke, runoff, or explosion risks could occur during a battery incident?
What cooling systems are required?
What fire suppression systems are required?
Do local emergency responders have the training and equipment needed?
How often will batteries be inspected, replaced, recycled, or disposed of?
Who is responsible for battery waste?

Fire Suppression

What fire suppression systems will be used?
Will the facility use water, foam, clean agents, inert gases, chemical systems, or specialized battery fire suppression?
What chemicals or gases will be stored on site?
Could fire suppression discharge affect workers, first responders, residents, animals, stormwater systems, groundwater, wetlands, rivers, or sewer systems?
How will accidental releases be prevented?
How will releases be reported?
Who is responsible for cleanup?
Will local emergency responders receive full information about suppression systems?

Refrigerants, Coolants, and Chemicals

What refrigerants will be used?
What coolants will be used?
What water-treatment chemicals will be used?
What cleaning chemicals, corrosion inhibitors, biocides, anti-scaling agents, dielectric fluids, or other substances will be used?
Where will chemicals be stored?
How will leaks be detected?
How will spills be contained?
How will chemicals be transported, replaced, and disposed of?
Do any substances have high global warming potential, toxicity, persistence, or aquatic impact?
Will a public chemical inventory be available?

Construction Emissions

How long will construction last?
Will construction occur in phases?
What diesel equipment will be used?

What truck traffic will be generated?
What dust controls will be required?
Will idling be restricted?
Will low-emission equipment be required?
Will construction emissions be monitored?
Will nearby homes, farms, schools, hospitals, care facilities, parks, and workers be protected?
Will construction routes avoid sensitive areas where possible?

Cumulative Impacts

Does the air assessment include full buildout?
Does it include future phases?
Does it include nearby roads, industry, substations, power plants, warehouses, or other data centers?
Does it include cumulative generator testing?
Does it include emergency operation of multiple facilities during the same grid event?
Does it include wildfire smoke or other existing regional air quality stressors?
Could this project contribute to an industrial air burden that no single approval captures?

Monitoring and Reporting

Will air quality be monitored after construction?
Will generator runtime be publicly reported?
Will generator testing be publicly reported?
Will fuel use be publicly reported?
Will emissions be measured or only estimated?
Will particulate matter, nitrogen oxides, and other relevant pollutants be monitored?
Will greenhouse gas emissions be reported annually?
Will incidents, spills, fire suppression releases, battery events, and emergency operations be reported in real time or near real time?
Who verifies the data?
Will data be independently audited?
What penalties apply if limits are exceeded?
Can operations be restricted if air impacts are greater than predicted?

Red Flags

An air, emissions, or backup-system proposal deserves greater scrutiny when the public hears:
"The facility will be powered by clean energy."
"Backup generators are only for emergencies."
"Emissions will be minimal."
"Generator testing will be routine."
"Air impacts will meet applicable standards."
"Battery storage is clean."
"Fire suppression systems are safe."
"Chemical details are commercially sensitive."

"Construction impacts will be temporary."
"Greenhouse gas emissions will be offset."
"The project will be carbon neutral."
"Emergency operations are unlikely."

Clean energy claims do not erase diesel generators.
Battery storage does not erase fire risk.
Offsets do not erase local emissions.
A permit limit does not erase exposure.
Emergency systems are still industrial systems, and industrial systems require public scrutiny.

What Communities Should Ask For

Before approval, communities should ask for:
A full air quality assessment.
A backup power system inventory.
A generator and gas turbine emissions assessment.
A testing schedule and public reporting plan.
A fuel storage and spill prevention plan.
A greenhouse gas emissions assessment.
A battery safety and fire risk assessment.
A fire suppression chemical assessment.
A refrigerant, coolant, and chemical inventory.
A construction emissions and dust-control plan.
A cumulative air impact assessment.
A full-buildout emissions assessment.
An emergency operation emissions plan.

A monitoring plan for air quality, generator runtime, fuel use, emissions, battery incidents, and chemical releases.

Real-time or near-real-time public reporting for testing, emergency operation, exceedances, spills, fires, and other incidents.

Independent auditing of emissions and incident data.

Clear penalties, operating restrictions, mitigation requirements, and permit-review triggers if air impacts exceed predictions.

The Public Interest Standard

No data center should be approved until the public understands the facility's air emissions, backup systems, fuel storage, battery risks, fire suppression systems, chemical use, testing schedules, emergency operations, and cumulative air impacts.

A community should not be asked to accept clean branding in place of clear evidence.

If a facility needs diesel generators, gas turbines, battery systems, fuel tanks, chemicals, fire suppression systems, and emergency power to protect its servers, then the public has the right to ask

how those systems protect — or endanger — the people, animals, land, air, water, and communities around them.

Digital infrastructure still breathes into the physical world.

The public has the right to know what it is breathing.

11 - Animals, Plants, Agriculture, and Ecosystems

A data center does not arrive alone.

It arrives with buildings, roads, fences, lights, cooling systems, power lines, substations, generators, batteries, drainage changes, water demand, heat rejection, traffic, noise, vibration, air emissions, stormwater runoff, construction disturbance, and long-term maintenance activity.

Each of these may be assessed separately in a technical report.

Animals, plants, farms, and ecosystems experience them together.

A wetland does not experience "stormwater" separately from heat, light, noise, sediment, road salt, water withdrawal, and habitat fragmentation. A herd of cattle does not experience generator testing separately from low-frequency sound, traffic, vibration, lighting, heat stress, air quality, and water competition. A pollinator does not experience a project according to municipal zoning categories. A stream does not divide its response according to which department issued which permit.

For this reason, the public should ask not only whether a data center affects people.

It should ask whether the project affects the living systems that surround and support the community.

Agriculture, wildlife, plants, wetlands, forests, grasslands, rivers, soil, pollinators, birds, amphibians, aquatic life, and livestock are not secondary concerns. They are part of the public interest.

Ecosystems Are Not Empty Space

Development proposals often describe land in terms of ownership, zoning, and availability.

But land is also habitat.

A field may feed people. A wetland may filter water. A roadside ditch may support amphibians. A hedgerow may shelter birds. A grassland may store carbon. A forest edge may provide movement cover. A pond may support insects, bats, and breeding species. Soil may hold decades of biological life. A farm may support livestock, crops, pollinators, drainage systems, and local food security.

When a data center is proposed, the public should ask what living systems are already there.

What animals move through the site?

What plants grow there?

What crops are produced nearby?

What wetlands, waterways, forests, grasslands, or soil systems may be affected?

What species use the site seasonally, at night, during migration, or during breeding?

What ecosystem functions may be lost even if no protected species is identified?

The absence of a rare species does not mean the absence of ecological value.

Livestock and Farm Animals

Livestock can be affected by changes in sound, vibration, light, heat, air quality, water access, traffic, and stress.

Cattle, horses, sheep, goats, poultry, pigs, and other animals may respond differently to construction noise, continuous mechanical hum, low-frequency vibration, nighttime lighting, truck traffic, generator testing, air emissions, dust, and changes in water availability. Farm animals may also be affected indirectly if roads are disrupted, pastures are fragmented, fences are altered, water systems are stressed, or farm routines are interrupted.

The public should not assume that livestock impacts are irrelevant simply because animals are not human residents.

Agriculture is a livelihood. Animal welfare matters. Food systems matter. Rural communities matter.

A data center proposed near farms should include a livestock and farm-impact assessment. That assessment should consider breeding, calving, lambing, foaling, poultry production, grazing, water access, feeding routines, barn ventilation, stress behaviour, productivity, veterinary needs, and emergency access.

If a project is near livestock operations, the public should ask whether farmers were consulted before the site was chosen, not after the project was already moving toward approval.

Crops, Soil, and Agricultural Production

A data center may affect crops even if it does not directly occupy an entire farm.

Construction can compact soil, alter drainage, increase dust, disrupt irrigation, change access routes, and fragment fields. Roads, substations, transmission lines, fencing, and drainage works can make farm operations more difficult. Heat, altered airflow, runoff, light, dust, water competition, or changes in local hydrology may affect nearby growing conditions.

Soil is not simply dirt waiting to be paved.

Healthy soil supports food production, carbon storage, water retention, microorganisms, fungi, insects, roots, and long-term agricultural resilience. Once soil is compacted, contaminated, excavated, or sealed under buildings and pavement, its function may be diminished for generations.

A data center proposal on or near farmland should assess crop impacts, soil quality, drainage, irrigation, access, dust, runoff, and long-term agricultural viability.

The public should ask whether the project removes farmland from production, weakens nearby farms, or creates pressure for further conversion of agricultural land.

Pollinators and Insects

Pollinators are essential to food systems and ecosystems.

Bees, butterflies, moths, flies, beetles, wasps, and other insects may be affected by habitat loss, pesticide or chemical exposure, light pollution, vegetation removal, heat, altered flowering patterns, dust, traffic, and changes in water availability. Night lighting can affect moths and other nocturnal insects. Loss of native plants can reduce forage. Heat islands can alter local plant and insect relationships.

A data center may not look like a pollinator issue at first glance.

But when open land, wetlands, hedgerows, fields, grasslands, or native vegetation are replaced with buildings, pavement, gravel, fencing, lighting, and mechanical equipment, pollinator habitat can be lost or fragmented.

The public should ask whether pollinator habitat has been mapped, whether native vegetation will be protected, whether landscaping will support local species, and whether lighting will be designed to reduce insect disruption.

Mitigation should not mean a few ornamental shrubs near the entrance.

If habitat is lost, replacement should be ecologically meaningful, maintained over time, and monitored.

Birds, Bats, and Migration

Birds and bats may be affected by light, noise, habitat loss, collision risks, insects, tree removal, water changes, and disruption of migration or feeding routes.

Artificial light can disorient migratory birds. Continuous noise may affect communication, nesting, feeding, predator avoidance, and breeding behaviour. Vegetation clearing may remove nesting habitat. Wetland disturbance may affect waterfowl and shorebirds. Changes in insect populations may affect bats and insectivorous birds.

The public should ask whether bird and bat assessments were conducted across appropriate seasons, including migration, breeding, nesting, and nighttime activity.

A single daytime site visit is not enough.

If the project includes tall structures, lighting, reflective surfaces, transmission lines, fencing, or large buildings near habitat corridors, the public should ask how collision, disorientation, and habitat fragmentation will be prevented.

Amphibians, Reptiles, and Small Wildlife

Amphibians are often early indicators of environmental stress.

Frogs, toads, salamanders, turtles, snakes, and other small wildlife may be affected by wetlands loss, road mortality, drainage changes, water contamination, sediment, noise, vibration, light, heat, and changes to breeding pools or seasonal movement routes.

These species may be easy to overlook because they are small, seasonal, nocturnal, or active during specific weather conditions.

A data center proposal should assess wetlands, temporary pools, ditches, riparian areas, culverts, and movement corridors. It should also consider construction timing, road crossings, stormwater systems, fencing, and lighting.

A project that appears to avoid a wetland may still harm amphibians if it cuts off the path between upland habitat and breeding pools.

Aquatic Life and Waterways

Aquatic ecosystems can be affected by water withdrawal, discharge, thermal pollution, stormwater runoff, sediment, road salt, chemicals, fuel spills, altered groundwater, reduced flows, increased temperature, and construction activity.

Fish, amphibians, aquatic insects, mussels, algae, plants, and microorganisms may all be affected by changes in water quantity or quality.

The public should ask whether the project affects rivers, streams, lakes, wetlands, ponds, ditches, groundwater, floodplains, or drainage systems. It should also ask whether low-flow conditions, drought, summer heat, winter conditions, and cumulative watershed impacts were assessed.

Water impacts should not be evaluated only at the pipe, ditch, or discharge point.

They should be evaluated downstream.

Wetlands, Forests, Grasslands, and Habitat Networks

Wetlands, forests, grasslands, riparian areas, and native vegetation provide more than scenery.

They regulate water, store carbon, cool the landscape, support biodiversity, reduce flooding, provide habitat, stabilize soil, shelter pollinators, and connect larger ecological networks.

A data center may affect these systems through direct removal, fragmentation, altered drainage, lighting, noise, heat, air emissions, roads, fencing, transmission corridors, and future expansion.

The public should ask whether the ecological assessment examines the full habitat network, not only the parcel boundary.

A wetland buffer may be too narrow. A forest patch may be cut off. A grassland may be divided by fencing. A wildlife corridor may be narrowed until it no longer functions. A stream may remain physically present but ecologically degraded.

Ecosystem function matters, not just mapped features.

Fencing, Barriers, and Fragmentation

Data centers often require secure perimeters.

Fencing, walls, gates, berms, lighting, patrol roads, and restricted access may be necessary for security, but they can also fragment habitat, block wildlife movement, alter drainage, and change how animals use the landscape.

A fence may protect equipment while cutting off migration routes, separating animals from water, trapping wildlife in road corridors, or increasing pressure on remaining habitat.

The public should ask whether wildlife movement has been assessed and whether fencing can be designed to reduce harm. That may include wildlife passages, setbacks, unfenced buffers, dark corridors, vegetation corridors, seasonal restrictions, or alternative site layouts.

Security should not become an excuse to ignore ecological connectivity.

Noise, Vibration, and Light as Ecological Impacts

Noise, vibration, and light are not only human nuisances.

They can change animal behaviour, alter habitat use, affect breeding, disrupt communication, interfere with predator-prey relationships, disorient birds and insects, and reduce the quality of otherwise intact habitat.

A wetland beside a loud, brightly lit mechanical yard is not the same habitat it was before.

The public should ask whether ecological assessments include continuous nighttime operation, low-frequency sound, generator testing, construction vibration, lighting, heat, and cumulative disturbance.

If the only ecological question asked is whether land is physically cleared, the assessment is incomplete.

Heat, Microclimates, and Plant Life

Heat can affect plant life, soil moisture, insects, livestock, wildlife, and local growing conditions.

A data center may create or worsen localized heat island effects through buildings, paving, roofs, mechanical equipment, heat rejection, reduced vegetation, and altered airflow. This may affect nearby crops, native plants, pollinator timing, tree stress, soil drying, livestock comfort, and habitat quality.

The public should ask whether local heat effects have been assessed for farms, gardens, forests, wetlands, grasslands, riparian areas, and wildlife habitat.

Plants are not passive scenery. They are living infrastructure.

Chemicals, Spills, and Runoff

Data centers may involve fuels, coolants, refrigerants, water-treatment chemicals, cleaning agents, fire suppression substances, transformer oils, battery materials, road salt, construction materials, and other industrial substances.

Even when these materials are properly managed, accidents can happen. Spills, leaks, fires, runoff, contaminated stormwater, and emergency releases can affect soil, water, plants, livestock, wildlife, and downstream ecosystems.

The public should ask for a chemical inventory, spill prevention plan, stormwater plan, emergency response plan, and ecological risk assessment.

A project should not be treated as low risk simply because its primary product is computation.

Its support systems are industrial.

Cumulative Ecological Disruption

One data center may remove a limited area of habitat.

Several data centers, roads, substations, transmission corridors, water withdrawals, construction phases, and industrial expansions may transform an entire landscape.

Cumulative ecological disruption can occur when each project is assessed separately and approved one at a time. By the time the total effect is visible, the habitat network may already be fragmented, water systems stressed, farmland converted, wildlife displaced, and rural character permanently altered.

The public should ask whether the assessment includes full buildout, future phases, nearby developments, regional data center clustering, transmission corridors, water infrastructure, transportation upgrades, and other reasonably foreseeable impacts.

The question is not only what this project does.

The question is what pattern this project begins.

Monitoring After Approval

Pre-approval ecological studies are not enough.

Animals move. Plants change. Wetlands respond over time. Crops vary by season. Livestock behaviour may shift after construction. Pollinators may decline slowly. Runoff problems may appear during storms. Heat effects may become visible in drought. Noise and light impacts may be clearer after nighttime operation begins.

For this reason, ecological monitoring should continue after approval and after operations begin.

Monitoring should include livestock impacts where farms are affected, pollinator habitat, bird and bat activity, amphibian movement, aquatic health, water quality, soil health, vegetation survival, invasive species, wetland function, wildlife movement, and complaints from farmers or residents.

Monitoring should be public, long-term, independent where necessary, and tied to enforceable remedies.

If the project causes more harm than predicted, approval conditions should be reopened.

Core Questions

Existing Ecological Conditions

What animals, plants, crops, wetlands, forests, grasslands, waterways, soils, and habitats are present on or near the site?

Were surveys conducted across appropriate seasons?

Were nighttime species considered?

Were breeding, nesting, migration, calving, lambing, foaling, and growing seasons considered?

Were Indigenous ecological knowledge, local farm knowledge, and community observations included?

Was the assessment limited to the project parcel, or did it include the broader ecosystem and watershed?

Livestock and Farm Animals

Are livestock operations located nearby?

What species are present?

Could sound, vibration, light, traffic, heat, air emissions, water competition, or construction affect them?

Have breeding, calving, lambing, foaling, poultry production, grazing, barn ventilation, and animal stress been assessed?

Were farmers and ranchers consulted?

Will livestock behaviour, reproduction, health, or productivity be monitored after construction?

Who is responsible if impacts occur?

Crops, Soil, and Agriculture

Will farmland be removed from production?

Will nearby crop production be affected?

What soil types and soil quality are present?

Will construction compact soil or alter drainage?

Will dust, runoff, heat, traffic, or water competition affect crops?

Will irrigation systems, farm access, drainage ditches, field operations, or harvest routes be disrupted?

Can the project be moved to lower-value or already-disturbed land?

Will agricultural impacts be monitored over time?

Pollinators and Insects

What pollinator habitat exists on or near the site?

Will native plants, hedgerows, field margins, wetlands, grasslands, or flowering areas be removed?

Will lighting affect nocturnal insects?

Will heat, dust, chemicals, or habitat loss affect pollinators?

Will landscaping use native plants?

Will pesticide use be restricted?

Will pollinator habitat be restored or expanded?

Who maintains and monitors pollinator habitat after construction?

Birds and Bats

Were bird and bat surveys completed during migration, breeding, nesting, and nighttime activity periods?

Will lighting disorient birds or insects that bats rely on?

Will vegetation clearing remove nesting habitat?

Will transmission lines, reflective surfaces, fencing, or buildings create collision risks?

Will noise affect communication, feeding, breeding, or habitat use?

Will bat roosts, wetlands, forest edges, grasslands, and migration corridors be protected?

Will monitoring continue after operation begins?

Amphibians, Reptiles, and Small Wildlife

Are wetlands, ponds, ditches, temporary pools, culverts, riparian areas, or seasonal movement routes present?

Will roads, fencing, drainage changes, stormwater systems, or construction block movement?

Will light, vibration, noise, heat, or water changes affect breeding or habitat?

Will construction be restricted during sensitive seasons?

Will wildlife crossings, buffers, or exclusion measures be required?

Will mortality be monitored after construction?

Aquatic Life

Will water withdrawal affect streams, rivers, lakes, wetlands, groundwater, or downstream flows?

Will discharge affect temperature, chemistry, sediment, or water quality?

Will stormwater runoff carry pollutants into aquatic systems?

Have low-flow, drought, summer heat, and cumulative watershed impacts been assessed?

Could fish, amphibians, aquatic insects, mussels, plants, algae, or microorganisms be affected?

Will aquatic monitoring occur upstream and downstream?

Will results be public?

Habitat and Connectivity

Does the site affect wildlife corridors, migration routes, riparian corridors, wetlands, forests, grasslands, or habitat networks?

Will fencing block animal movement?

Will roads increase wildlife mortality?

Will lighting create barriers for nocturnal species?

Will noise or vibration reduce usable habitat?

Will the project fragment habitat even if it avoids direct destruction?

Will ecological corridors be preserved, restored, or created?

Will future phases narrow or remove remaining corridors?

Noise, Light, Heat, and Air

Have ecological impacts from noise been assessed?

Have low-frequency sound and continuous nighttime operation been considered?

Have vibration impacts been assessed?

Have lighting impacts been assessed for birds, bats, insects, amphibians, livestock, and wildlife corridors?

Have heat island effects been assessed for plants, animals, crops, wetlands, and soil moisture?

Have air emissions from generators, traffic, construction, and fires been assessed for ecological impacts?

Chemicals, Runoff, and Spills

What fuels, coolants, refrigerants, fire suppression chemicals, water-treatment chemicals, battery materials, transformer oils, cleaning agents, and other substances will be used?

Could spills, leaks, fires, or runoff affect soil, water, crops, livestock, wildlife, wetlands, or aquatic life?

How will stormwater be collected, treated, and monitored?

Will runoff be tested after storms?

What happens if contaminated water leaves the site?

Who is responsible for cleanup?

Cumulative Impacts

Does the assessment include the full buildout?

Does it include future phases?

Does it include transmission lines, substations, roads, water infrastructure, stormwater systems, and construction staging?

Does it include nearby developments and other proposed data centers?

Could the project contribute to regional habitat fragmentation?

Could it contribute to farmland loss?

Could it contribute to watershed stress?

Could it create an industrial corridor where ecological impacts are assessed too narrowly?

Monitoring and Accountability

Will ecological monitoring continue after approval?
For how many years?
Who conducts the monitoring?
Will the monitoring be independent?
Will livestock, crops, pollinators, birds, bats, amphibians, aquatic life, soil health, wetlands, vegetation, and wildlife movement be included where relevant?
Will farmers, Indigenous communities, residents, and local naturalists be able to report impacts?
Will monitoring results be public?
What happens if impacts are greater than predicted?
Can operations be modified?
Can lighting be reduced?
Can noise mitigation be strengthened?
Can water use be restricted?
Can habitat restoration be required?
Can permits be reopened?

Red Flags

An animals, plants, agriculture, or ecosystems proposal deserves greater scrutiny when the public hears:
"No significant species were identified."
"The land is currently unused."
"The site is mostly open field."
"Impacts will be mitigated."
"Wildlife can move around the project."
"Lighting impacts will be minimal."
"Noise impacts are within standards."
"Construction impacts will be temporary."
"Stormwater will be managed through standard practices."
"Habitat loss is limited to the project footprint."
"Future phases will be assessed later."
"Agricultural impacts are not expected."

Open field is not empty.
A wetland buffer is not protection if the water system changes.
A wildlife corridor is not preserved if it no longer functions.
A farm is not unaffected because the building sits next door instead of directly on top of it.

What Communities Should Ask For

Before approval, communities should ask for:
A full ecological impact assessment.
A livestock and agricultural impact assessment where farms are nearby.

A soil and crop impact assessment where agricultural land may be affected.

A pollinator and native plant assessment.

Bird and bat surveys across appropriate seasons.

Amphibian, reptile, and small wildlife assessments where wetlands, ponds, ditches, or corridors are present.

An aquatic life and waterway impact assessment.

A wetland, forest, grassland, and habitat connectivity assessment.

A wildlife corridor and fencing impact assessment.

A noise, vibration, light, heat, and air impact assessment for animals and ecosystems.

A chemical, spill, runoff, and stormwater ecological risk assessment.

A cumulative ecological impact assessment including full buildout and future phases.

A habitat protection, restoration, and monitoring plan.

A construction timing plan that avoids sensitive breeding, nesting, migration, and farm production periods where possible.

A long-term public ecological monitoring plan.

Legally enforceable mitigation, restoration, reporting, and penalty provisions.

Clear permit-review triggers if ecological impacts exceed predictions.

The Public Interest Standard

No data center should be approved until the public understands how the project may affect livestock, crops, soil, pollinators, birds, bats, amphibians, aquatic life, wetlands, forests, grasslands, wildlife corridors, and ecosystem function.

The living world around a data center should not be treated as scenery around a server farm.

Agriculture is infrastructure.

Pollinators are infrastructure.

Wetlands are infrastructure.

Soil is infrastructure.

Wildlife corridors are infrastructure.

Ecosystems are infrastructure.

A community that protects only the building and not the living systems around it has misunderstood what is being built.

The public has the right to ask whether a data center can exist in a place without making that place less alive.

12 - Cumulative Impacts

A single data center proposal may be presented as manageable.

One building.

One site.

One water connection.

One grid connection.

One road upgrade.

One substation.

One set of permits.

One environmental review.

One tax agreement.

One public hearing.

But communities do not experience development one permit at a time.

They experience the accumulation.

One data center can become a campus. One campus can become a corridor. One corridor can become an industrial cluster. One substation can invite more load. One transmission line can enable more projects. One water allocation can become the precedent for the next. One road upgrade can open nearby land to further development. One tax incentive can become the baseline for future negotiations.

The public should not ask only whether one project can be managed.

The better question is whether the buildout pattern can be managed.

Cumulative impacts are the combined effects of existing, proposed, approved, reasonably foreseeable, and enabled developments. They include the impacts of the data center itself, but also the infrastructure required to support it: transmission corridors, substations, water withdrawals, pipelines, roads, cooling systems, backup generators, fuel storage, stormwater systems, sewer expansions, battery installations, land clearing, industrial zoning, and future phases.

A data center should never be assessed as though it exists alone when it is clearly part of a larger pattern.

The Problem With Project-by-Project Approval

Project-by-project approval can make large transformations appear small.

Each proposal may claim its impacts are limited. Each may say water use is manageable. Each may say the grid can accommodate the load. Each may say traffic impacts are acceptable. Each may say wildlife impacts are mitigated. Each may say noise remains within standards. Each may say emissions are minimal. Each may say future phases will be reviewed later.

But by the time all of those small approvals are added together, the community may be living with something much larger than what the public was originally asked to consider.

A region may lose farmland piece by piece.

A watershed may be stressed allocation by allocation.

A grid may be burdened connection by connection.

A quiet rural area may become industrialized facility by facility.

A wildlife corridor may be narrowed project by project until it no longer functions.

A tax base may be reshaped incentive by incentive.

A public utility may be converted into a private growth engine one agreement at a time.

Cumulative impact review exists because harm does not need to arrive all at once to be real.

The First Project Is Often the Most Important

The first data center in a region may be treated as a test case.

But in many ways, the first project is the most important one.

It creates precedent. It establishes the political language. It normalizes the land use. It introduces specialized infrastructure. It may justify new transmission capacity, larger water systems, road improvements, emergency planning changes, and industrial zoning. It may encourage land speculation. It may attract other developers. It may shift how governments imagine the future of the region.

Once the first facility is approved, future proposals may be described as logical, efficient, or inevitable because the infrastructure is already there.

This is why the public must ask not only:

What does this project require?

But also:

What does this project make possible?

A development that appears modest today may be the anchor for a much larger industrial system tomorrow.

Full Buildout Must Be Assessed

A data center proposal should be evaluated at full buildout.

If the project includes phases, future buildings, reserved land, expandable power capacity, oversized water infrastructure, scalable cooling systems, additional generators, or future tenants, those possibilities should be included in the review.

The public should not be asked to approve the first phase while being told the rest will be assessed later, especially if the first phase creates the infrastructure that makes later phases difficult to refuse.

Full buildout means asking what the site, campus, corridor, or region could reasonably become under the approvals, infrastructure, zoning, contracts, and land assembly being put in place.

It also means asking whether the public would still support the first approval if the full pattern were visible from the beginning.

Infrastructure as a Growth Signal

Infrastructure does not merely serve development.

It can attract it.

A new substation may make nearby land more valuable for energy-intensive users. A transmission upgrade may enable future data centers. A water pipeline may create capacity for industrial clustering. A widened road may open rural land to logistics, warehouses, or more data infrastructure. A sewer expansion may make future development easier. A gas line may support backup generation or on-site power. A fiber route may attract additional digital infrastructure.

For this reason, infrastructure should be assessed not only as a response to the proposed project, but as a signal of future development.

The public should ask whether infrastructure is being sized for the current proposal, future phases, additional data centers, or a larger industrial strategy.

If the infrastructure is larger than the current project requires, the public has the right to know why.

Water Cumulative Impacts

Water impacts can accumulate quietly.

One data center may claim modest water use. A second may use reclaimed water. A third may draw from groundwater. A fourth may rely on municipal supply. Another may require emergency water during heat waves. Another may discharge treated or heated water. Each may appear manageable on its own.

Together, they may reshape a watershed.

Cumulative water review should include withdrawals, consumption, discharge, thermal pollution, stormwater, groundwater drawdown, aquifer recharge, drought conditions, downstream flows, wetlands, agriculture, Indigenous rights, ecosystem needs, future housing, and climate change.

The public should ask whether the watershed can support the total demand, not only the first application.

Water should not be allocated by whoever arrives first with the largest promise.

Electricity Cumulative Impacts

Grid impacts also accumulate.

One data center may require a substation. Several may require transmission expansion. A cluster may require new generation, new reserve capacity, new grid controls, new backup systems, and major public investment. Each project may claim its own connection is manageable, while the combined load reshapes the entire regional grid.

Cumulative electricity review should include all existing and proposed data centers, full-buildout demand, substations, transmission corridors, distribution upgrades, backup generation, battery systems, ratepayer costs, grid reliability, renewable energy availability, fossil generation, emergency curtailment, and public priority during grid stress.

The public should ask whether the grid is being planned for public need or reorganized around private load growth.

Land and Habitat Cumulative Impacts

Land-use impacts can be hard to reverse once they begin.

A single facility may remove a limited amount of land. But a cluster of data centers, roads, substations, transmission lines, fences, stormwater ponds, fuel storage areas, and utility corridors may transform an entire landscape.

Cumulative land review should include farmland loss, habitat fragmentation, wetland impacts, forest clearing, grassland conversion, wildlife corridors, visual character, future housing conflicts, Indigenous land use, agricultural viability, and regional planning.

The public should ask whether the project contributes to a development pattern that the community would reject if it were proposed all at once.

Noise, Light, Heat, and Air Cumulative Impacts

Noise, light, heat, and air emissions can combine in ways that single-project assessments miss.

One mechanical yard may be tolerable. Several may create continuous industrial sound. One facility's lighting may be manageable. Several may erase dark skies. One heat source may be minor. A cluster may contribute to a local heat island. One generator test may be limited. Dozens of generators across several facilities may create recurring noise and emissions. One facility's construction may be temporary. Repeated phased construction may make disruption nearly permanent.

Cumulative assessment should include all existing and foreseeable sources of sound, vibration, lighting, heat rejection, air emissions, generator testing, traffic, and construction.

The public should ask whether the total lived environment remains acceptable.

A community should not be told each separate impact is small while the combined effect changes the character of the place.

Industrial Clustering and Community Identity

Data centers may attract more than servers.

They may attract substations, power plants, battery storage, gas infrastructure, fiber routes, warehouses, cooling plants, security zones, industrial roads, transmission corridors, and speculative land development. Over time, an area may shift from rural, agricultural, residential, mixed-use, or ecological land into an industrial technology corridor.

That may be a deliberate planning choice in some places. But it should be made openly.

The public should ask whether governments are approving a single data center or quietly creating a regional industrial strategy without naming it.

If the goal is to build a data center cluster, the public deserves a regional plan, cumulative assessment, infrastructure strategy, environmental review, public consultation process, Indigenous consultation process, and public cost analysis that reflect that larger intention.

Industrial transformation should not happen by accident.

The Problem of Split Jurisdiction

Cumulative impacts are often missed because authority is divided.

A municipality may approve land use. A province or state may approve water licences. A utility regulator may approve grid upgrades. An environmental agency may assess wetlands. A transportation department may approve roads. A federal agency may review endangered species, navigable waters, Indigenous consultation, or emissions. Each body may look at its own piece.

The public experiences the whole project.

A cumulative impact process should connect the pieces across jurisdictions. It should identify who is responsible for seeing the full picture and who has the authority to say no, pause, redesign, or require stronger conditions when the combined burden becomes too high.

A project should not be allowed to escape scrutiny because every regulator is looking at only one slice of the same elephant.

Time Matters

Cumulative impacts unfold over time.

Construction may last years. Future phases may be added later. Water use may rise as workloads increase. Electricity demand may grow as computing density increases. Cooling systems may change. Tenants may change. AI workloads may increase power and heat demand. Nearby land may be developed. Climate conditions may worsen. Infrastructure may age. Promises made during approval may become difficult to enforce a decade later.

The public should ask whether the review considers the life of the facility, not only the opening day.

A data center built today may affect a region for thirty or forty years. Its cumulative impact should be assessed over that same horizon.

Growth Caps and Trigger Points

If cumulative impacts are uncertain, approvals should include clear limits.

A community may decide that one facility is acceptable but ten are not. It may decide that the first phase is acceptable but expansion requires new review. It may decide that water use must be capped. It may decide that grid demand cannot increase without public approval. It may decide that additional substations, generators, or cooling systems trigger a new cumulative assessment.

These limits should be written into approvals.

Growth caps and trigger points may include maximum power demand, maximum water use, maximum heat rejection, maximum generator capacity, maximum building area, maximum nighttime sound, maximum discharge, maximum traffic, maximum land disturbance, maximum emissions, and mandatory review before future phases.

Without enforceable limits, cumulative impact review becomes a description rather than a safeguard.

Core Questions

Buildout Pattern

Is this project a single facility or part of a larger campus?

Are future phases planned?

Are future phases implied by land assembly, oversized infrastructure, zoning, utility agreements, or road design?

What is the maximum buildout possible?

What other data centers are proposed, approved, operating, or being discussed in the region?

Could this project become the anchor for a data center corridor or industrial cluster?

Would the public evaluate the project differently if the full buildout were presented today?

Infrastructure

What transmission lines, substations, transformers, distribution upgrades, water lines, sewer systems, roads, bridges, pipelines, stormwater systems, fiber routes, cooling plants, backup systems, or fuel infrastructure are required?

Are these upgrades sized only for the current project?

Are they sized for future phases?

Are they sized for additional data centers or industrial users?

Who pays for each piece of infrastructure?

Who benefits from the excess capacity?

Will public infrastructure built for this project make future industrial development more likely?

Water

What is the cumulative water demand of this project, future phases, nearby data centers, and other industrial users?

What is the cumulative withdrawal, consumption, and discharge?

Has the watershed been assessed under drought and climate-change scenarios?

Could cumulative water demand affect households, farms, Indigenous rights, wetlands, fisheries, aquatic life, downstream users, or future housing?

Will water allocations be capped?

Can future facilities receive water approvals before cumulative impacts are reviewed?

Electricity

What is the cumulative power demand of all existing, approved, proposed, and reasonably foreseeable data centers in the region?

What is the full-buildout demand?

What grid upgrades are required across all projects?

What new generation may be required?

Will fossil generation or backup systems increase?

Will ratepayers absorb any costs?

Will local users face reliability risks?

Will the grid be planned around public need or private data center growth?

Can additional electrical load be approved without a new public review?

Land Use

How much land will be converted at full buildout?

How much farmland may be lost?

How much habitat may be fragmented?

How much wetland, forest, grassland, or open space may be affected?

Will roads, transmission lines, substations, fencing, and utility corridors divide the landscape?

Will future housing, schools, hospitals, farms, parks, or conservation areas be constrained?

Does the project align with regional planning, or does it create a new development pattern by default?

Noise, Light, Heat, and Air

What are the cumulative sound impacts of all facilities and supporting infrastructure?

What are the cumulative nighttime lighting impacts?

What are the cumulative heat island effects?

What are the cumulative air emissions from generators, gas turbines, construction, traffic, and backup systems?

What happens if multiple facilities test generators in the same period?

What happens if multiple facilities run backup systems during the same grid emergency?

What happens if multiple facilities expand at the same time?

Transportation

What cumulative construction traffic will result from this project and related developments?

Will roads, bridges, intersections, farm routes, school bus routes, emergency routes, or local businesses be affected?

Will road upgrades encourage additional development?

Will the community face years of rolling construction?

Who pays for cumulative transportation impacts?

Ecosystems

What cumulative ecological impacts will result from the project, future phases, infrastructure, and nearby developments?

Will wildlife corridors remain functional?

Will wetlands remain connected?

Will farms remain viable?

Will pollinator habitat be preserved?

Will aquatic systems remain healthy?

Will noise, light, heat, water withdrawals, discharge, and habitat fragmentation be assessed together?

Public Finance

What are the cumulative public subsidies, tax incentives, discounted utility rates, grants, loans, infrastructure costs, and maintenance obligations connected to data center development in the region?

What is the total public cost per permanent job?

What is the total public cost per unit of tax revenue?

Will public finances be exposed if projects are delayed, sold, automated, abandoned, or made obsolete?

Are clawbacks, bonds, or cost-recovery agreements in place?

Governance

Who is responsible for assessing cumulative impacts?

Which level of government sees the full picture?

Are municipal, provincial/state, federal, utility, water, transportation, environmental, and Indigenous consultation processes connected?

Can approvals be paused until cumulative impacts are assessed?

Are there regional caps, thresholds, or trigger points?

Will the public receive a cumulative impact report before approval?

Monitoring and Accountability

Will cumulative impacts be monitored over time?

Will water use, power demand, emissions, noise, light, heat, traffic, ecological impacts, and public costs be reported across all facilities?

Will data be public and updated regularly?

Will cumulative thresholds trigger new reviews or restrictions?

Can approvals be reopened if regional impacts exceed predictions?

Will future phases be automatically approved, or will they require full public review?

Red Flags

A cumulative impact proposal deserves greater scrutiny when the public hears:

"This application is only for the first phase."

"Future phases will be assessed later."

"This project should be considered on its own merits."

"Regional impacts are outside the scope of this review."

"Grid upgrades will be handled separately."

"Water approvals are a separate process."

"Traffic impacts are temporary."

"Only a small portion of the land is being developed now."

"The infrastructure may also support future growth."

"Other data centers are not part of this application."

"Cumulative impacts are not expected to be significant."

"Existing regulatory processes are sufficient."

Separate approvals do not create separate realities.

A watershed does not care which permit came first.

A grid does not care which company submitted which application.

A wildlife corridor does not care where one property line ends and another begins.

A community does not live inside the boundaries of a technical review.

What Communities Should Ask For

Before approval, communities should ask for:

A full cumulative impact assessment.

A full-buildout assessment.

A regional data center development map.

A map of existing, proposed, approved, and reasonably foreseeable data centers.

A map of required transmission, substation, water, sewer, road, pipeline, fiber, cooling, and backup infrastructure.

A cumulative water demand and discharge assessment.

A cumulative grid demand and ratepayer impact assessment.

A cumulative land-use and farmland conversion assessment.

A cumulative habitat and wildlife corridor assessment.

A cumulative sound, light, heat, and air assessment.

A cumulative transportation and construction disruption assessment.

A cumulative public subsidy and infrastructure cost assessment.

A regional emergency services impact assessment.

A climate-change scenario assessment.

A public finance risk assessment.

A governance map showing which agencies approve which parts of the development.

Clear growth caps and trigger points.

Mandatory public review before future phases.

Public reporting of cumulative impacts over time.

Independent auditing of cumulative impact data.

Legally enforceable limits, penalties, mitigation requirements, and permit-review triggers if cumulative impacts exceed predictions.

The Public Interest Standard

No data center should be approved until the public understands not only the project, but the pattern it may create.

A community should not be asked to approve one building while governments and industry quietly prepare the infrastructure for ten.

A single approval can become a corridor.

A corridor can become a cluster.

A cluster can become a new industrial identity for an entire region.

If that is the plan, the public deserves to hear it plainly.
Cumulative impact review is not obstruction.
It is honesty at the correct scale.

Part Three: Data, Power, and Sovereignty

13 - Data Sovereignty

A data center is not only a physical building.

It is also a jurisdictional space.

The land may be local. The water may be local. The electricity may be local. The roads, emergency services, tax incentives, and public infrastructure may be local. But the data inside the facility may be controlled by companies, clients, parent corporations, cloud providers, governments, investors, or legal systems located somewhere else.

That distinction matters.

A data center can be built in one country, province, state, municipality, or Indigenous territory while being owned, operated, financed, controlled, or accessed through another jurisdiction. The public may be told that the data center is "local" because the building is local. But data sovereignty is not guaranteed by geography.

The public should not ask only:

Where is the data center located?

The better question is:

Who controls the data, what laws apply, who can access it, and whose sovereignty is being respected or weakened?

Data Sovereignty Is More Than Data Location

Data sovereignty is often reduced to the question of where data is stored.

That is not enough.

Where data is stored matters, but so do ownership, corporate structure, contracts, encryption, access rights, technical control, cloud architecture, parent-company obligations, subcontractors, foreign laws, law-enforcement requests, intelligence access, public-sector procurement, and the ability of governments or communities to enforce their own rules.

A data center may store data inside a country while the company operating it is headquartered elsewhere. The servers may be owned by one entity, the building by another, the land by another, and the cloud service by another. The client may be a foreign corporation. The parent company may be subject to foreign legal demands. The technical administrators may operate from another country. The encryption keys may be controlled outside the jurisdiction. Backup copies may be stored elsewhere. Disaster recovery systems may replicate data across borders.

A local building does not automatically create local control.

The public should ask whether the proposed data center strengthens data sovereignty or merely creates the appearance of it.

Foreign Laws and Compelled Access

One of the most important questions is whether companies connected to the data center may be subject to foreign laws that compel data access.

In some countries, laws can require companies based there to comply with lawful information or data requests, even when the data is stored in another country. This means that a data center located locally may still be vulnerable to foreign legal processes if the owner, operator, cloud provider, parent company, or service provider is based in a jurisdiction with extraterritorial data-access powers.

This should be clearly understood before governments, schools, hospitals, courts, police services, public agencies, municipalities, Indigenous governments, or critical infrastructure providers place sensitive data in that facility or its cloud services.

The public should ask:

Can a foreign government compel access to data stored here?

Can a foreign court, law-enforcement agency, intelligence agency, or regulator require the company to produce data?

Can the company be ordered to provide data without notifying the local government, client, affected person, or public agency?

Can the company be prevented from disclosing that the request occurred?

Do local privacy laws override those foreign obligations, or do the foreign obligations still apply to the company?

If the answer is uncertain, that uncertainty is itself a public-interest concern.

Public-Sector Data

Public-sector data deserves special scrutiny.

If a data center will host, process, back up, mirror, analyze, or transmit government data, then the public has the right to know what kind of data is involved and what safeguards apply.

Public-sector data may include health records, school records, court records, policing data, social services files, tax records, municipal data, land titles, child welfare information, immigration information, public housing records, transportation data, emergency services data, utility data, environmental monitoring data, identity documents, procurement records, and communications between residents and governments.

This is not ordinary commercial information.

Public data is collected through public power. It is often mandatory. People cannot meaningfully opt out of needing health care, education, courts, utilities, emergency services, licences, benefits, permits, or public programs. Because the public is required to provide this information, governments have a heightened duty to protect it.

A government should not move public data into privately controlled or foreign-controlled infrastructure without explaining the sovereignty, privacy, access, accountability, and legal consequences.

Health, Education, Courts, Policing, and Social Services

Some categories of data require even greater caution.

Health data can reveal illness, disability, treatment, medication, mental health, reproductive care, addiction, genetics, and family history.

Education data can reveal children's identities, learning needs, behaviour, attendance, disabilities, family circumstances, and disciplinary records.

Court and policing data can reveal allegations, investigations, victim information, witness information, criminal records, family disputes, restraining orders, immigration status, and legal vulnerabilities.

Social service data can reveal poverty, disability, housing instability, child protection involvement, domestic violence risk, and personal crisis.

These kinds of data should not be treated as ordinary files in a cloud service.

If a data center will store or process sensitive public-sector data, the public should ask whether the facility, operator, parent company, cloud provider, subcontractors, and legal structure meet the highest standard of sovereignty, privacy, security, transparency, and democratic accountability.

Indigenous Data Sovereignty

Indigenous data sovereignty must not be treated as a footnote.

Indigenous governments, Nations, communities, and peoples have rights, laws, responsibilities, governance systems, knowledge systems, and relationships to land, water, culture, language, health, membership, children, ancestry, sacred sites, harvesting, and traditional knowledge that may be affected by data collection, storage, processing, and control.

Data about Indigenous people, lands, waters, resources, health, education, children, languages, cultural practices, traditional knowledge, ecological knowledge, and governance should not be extracted, hosted, analyzed, or commercialized without Indigenous authority, consent, and control.

If a data center is built on or near Indigenous territory, relies on resources connected to Indigenous rights, or hosts data involving Indigenous peoples or governments, then the question is not only whether general privacy law is followed.

The question is whether Indigenous data sovereignty is respected.

That includes asking who controls the data, who defines permitted use, who benefits, who has access, where data is stored, how it may be transferred, how it may be deleted, and whether Indigenous laws, protocols, and governance decisions are binding.

Municipal, Provincial, State, and National Sovereignty

Data sovereignty also matters for municipalities, provinces, states, and national governments.

A municipality may approve a data center hoping for local development, only to discover that the facility serves external corporate or foreign government interests while consuming local infrastructure and resources. A province or state may promote data center investment without knowing whether it creates dependence on foreign-owned cloud platforms. A national government may encourage digital infrastructure while critical public services become reliant on companies subject to another country's laws.

The public should ask whether data center development is building genuine local capacity or deepening dependence on external digital systems.

If public institutions cannot operate without foreign-owned cloud services, if local data cannot be audited locally, if emergency systems depend on remote corporate platforms, or if public agencies cannot change providers without major disruption, then sovereignty has been weakened even if the servers sit nearby.

A data center can be physically domestic and politically dependent.

Ownership, Control, and Corporate Structure

Data sovereignty cannot be assessed without knowing who controls the facility.

A data center may involve multiple layers of ownership: landowner, developer, building owner, operator, cloud provider, tenant, parent company, financing partner, real estate investment trust, subcontractor, equipment vendor, security contractor, and managed service provider.

Each layer may create different legal obligations, access rights, liabilities, and vulnerabilities.

The public should ask for a clear ownership and control map.

Who owns the land?
Who owns the building?
Who owns the servers?
Who operates the facility?
Who controls access?
Who controls encryption keys?
Who controls backups?
Who provides cloud services?
Who are the major tenants?
Where are the parent companies headquartered?

What foreign laws apply?
Who is liable if data is accessed, breached, transferred, misused, or compelled by another government?

If the public cannot understand who controls the facility, it cannot understand the sovereignty risk.

Cloud Architecture and Cross-Border Data Movement

Data may not remain in one building.

Cloud systems often rely on replication, redundancy, load balancing, backups, disaster recovery, remote administration, content delivery networks, software updates, support teams, subcontractors, and distributed processing.

A data center may be local, but the data may still move.

It may be mirrored in another region. It may be backed up across borders. It may be processed remotely. It may be accessed by technical staff in another country. It may be analyzed by AI systems elsewhere. It may pass through networks, vendors, platforms, or support systems that are not disclosed in a local land-use application.

The public should ask whether the facility guarantees data residency, data sovereignty, or both.

Data residency means data is stored in a particular place.

Data sovereignty means the data remains subject to the laws, governance, access rules, and control of the people or jurisdiction that should govern it.

Residency without sovereignty may not be enough.

Encryption and Key Control

Encryption is often used as a reassurance.

But encryption is only as strong as the control of the keys, the security of the systems, the legal obligations of the provider, and the circumstances under which access may be compelled.

The public should ask who controls encryption keys.

Are keys controlled by the client, the cloud provider, the data center operator, a foreign parent company, a third-party vendor, or a government agency? Can the provider access unencrypted data? Can the provider be compelled to assist in access? Are backups encrypted? Are logs encrypted? Are metadata protected? Can administrators access systems remotely?

A company should not be allowed to use the word "encrypted" as a substitute for explaining control.

If public-sector, Indigenous, health, education, legal, policing, or sensitive community data is involved, encryption and key control should be part of the sovereignty review.

Artificial Intelligence and Secondary Use

Data sovereignty also includes the question of secondary use.

Will data stored or processed in the facility be used to train, fine-tune, test, or operate artificial intelligence systems? Will metadata, behavioural data, public-service data, health data, student data, policing data, legal records, environmental data, or community data be used for analytics, prediction, profiling, automation, or commercial model development?

The public should ask whether data center infrastructure enables secondary uses that were never clearly approved by the people whose data is involved.

A person may consent to provide information for health care, school, court, public benefits, licensing, or municipal services. That does not mean they consent to the data being used for AI training, predictive modelling, commercial analytics, surveillance tools, or automated decision systems.

If the data center supports AI workloads, the public should ask not only what the facility consumes, but what the systems inside it are being trained or deployed to do.

Economic Development and Digital Dependency

Data center proposals are often presented as economic development.

But a community should ask whether the project builds local digital capacity or simply hosts infrastructure for external control.

Will local governments, schools, hospitals, businesses, researchers, or communities receive affordable access to computing capacity?

Will the facility create local technical employment, training, public digital infrastructure, or sovereign cloud capacity?

Will public institutions become dependent on a private provider?

Will public subsidies support infrastructure that local residents cannot meaningfully use?

Will the facility process local data while profits, control, and decision-making leave the region?

Economic development should not be measured only by construction value, tax revenue, or ribbon-cutting announcements.

It should also be measured by who controls the infrastructure after it is built.

Security, Breach, and Accountability

Data sovereignty is closely tied to accountability.

If data is breached, accessed, transferred, lost, seized, or misused, who is responsible? Which law applies? Which regulator investigates? Which court has authority? Which government is notified? Which people are informed? What penalties apply? Can affected individuals seek remedies? Can public agencies terminate contracts? Can data be returned, deleted, or migrated?

A local approval process should not ignore these questions simply because they are digital rather than physical.

If a data center receives public support, hosts public data, or becomes part of critical infrastructure, then breach and access accountability should be part of the public-interest review.

Core Questions

Data Categories

Whose data will be stored, processed, backed up, mirrored, transmitted, or analyzed in the facility?

Will the facility handle personal data?

Will it handle government data?

Will it handle health data?

Will it handle education data?

Will it handle court, policing, corrections, or legal data?

Will it handle social service data?

Will it handle Indigenous data, traditional knowledge, land-use data, health data, membership data, or governance data?

Will it handle biometric data, geolocation data, financial data, children's data, or identity documents?

Will the public be told what categories of data are involved?

Public-Sector Data

Will any municipal, provincial, state, federal, Indigenous, health, education, court, policing, emergency services, utility, or public-service data be hosted or processed?

Which public agencies will use the facility or its cloud services?

Are public-sector contracts already signed?

Are public agencies being encouraged or required to migrate to this infrastructure?

What procurement rules apply?

What privacy impact assessments have been completed?

Will public agencies be able to leave the provider without losing access, functionality, or control?

Ownership and Control

Who owns the land?

Who owns the building?

Who owns the servers?

Who operates the facility?

Who provides cloud services?

Who are the tenants?

Who controls physical access?

Who controls administrative access?

Who controls encryption keys?

Who controls backups?

Who controls logs and metadata?

Where are the owner, operator, cloud provider, parent company, and major tenants headquartered?

What foreign laws apply to each of them?

Foreign Legal Access

Can a foreign government compel the owner, operator, cloud provider, parent company, tenant, or service provider to provide access to data stored in the facility?

Can data be accessed under another country's court order, warrant, subpoena, intelligence process, national security law, or regulatory demand?

Can the company be prohibited from notifying the local client, government, affected person, or public?

Do local laws prevent foreign access, or can foreign obligations still apply to the company?

Has an independent legal analysis been completed?

Will that analysis be public?

Indigenous Data Sovereignty

Could the facility store, process, analyze, or transmit Indigenous data?

Could it involve data about Indigenous lands, waters, rights, health, education, children, languages, cultural knowledge, traditional knowledge, resources, governance, or membership?

Have Indigenous governments been consulted about data governance, not only land and water impacts?

Will Indigenous laws, protocols, consent requirements, and governance decisions apply?

Who controls access to Indigenous data?

Can Indigenous governments require deletion, return, restriction, localization, or audit of data?

Will Indigenous data be protected from unauthorized secondary use, AI training, commercial use, or foreign access?

Data Residency and Movement

Will data remain in the local jurisdiction?

Will data be mirrored, backed up, replicated, or processed elsewhere?

Will disaster recovery systems move data across borders?

Will remote administrators in other jurisdictions have access?

Will subcontractors or vendors outside the jurisdiction have access?

Will metadata, logs, diagnostics, or support data leave the jurisdiction?

Will the facility guarantee data residency, data sovereignty, or both?

Encryption and Technical Control

Will data be encrypted at rest?

Will data be encrypted in transit?

Who controls the encryption keys?

Can the provider access unencrypted data?

Can the provider be compelled to assist in access?

Are backups encrypted?

Are logs and metadata encrypted?

Can clients use customer-controlled keys?

Can public agencies use sovereign key management?

Can encryption arrangements be independently audited?

AI and Secondary Use

Will data in the facility be used for AI training, fine-tuning, inference, analytics, profiling, prediction, automation, surveillance, or commercial model development?

Will public-sector data be excluded from AI training?

Will health, education, policing, court, social service, Indigenous, children's, or biometric data be excluded from secondary use?

Will tenants be required to disclose AI-related uses?

Can clients prohibit secondary use?

Will metadata be used for analytics or training?

Can data be combined with other datasets?

Who audits compliance?

Critical Infrastructure and Dependency

Will the facility support critical public services?

Will it host emergency services, health systems, schools, courts, policing, utilities, transportation, water systems, energy systems, or government operations?

Would a failure, breach, foreign order, corporate dispute, bankruptcy, or service termination affect public services?

Is there a public exit plan?

Can data and services be migrated to another provider?

Will local institutions become dependent on foreign-owned digital infrastructure?

Will public money create private digital lock-in?

Accountability and Remedies

Who is liable if data is breached, accessed, transferred, seized, lost, misused, or used beyond its approved purpose?

Which regulator investigates?

Which court has jurisdiction?

Which law applies?

Who must be notified?

How quickly must notice be given?

What penalties apply?

Can public contracts be terminated?

Can data be returned or deleted?

Can affected individuals seek remedies?

Will audit results be public?

Red Flags

A data sovereignty proposal deserves greater scrutiny when the public hears:

"The data will be stored locally."

"The facility will comply with all applicable laws."

"The company follows industry-leading security standards."

"Data is encrypted."
"Tenants are confidential."
"Corporate structure is commercially sensitive."
"Public-sector clients have not been finalized."
"Data may be replicated for resilience."
"Foreign access is unlikely."
"Legal requests are handled through normal processes."
"AI use depends on customer needs."
"Security details cannot be disclosed."

Local storage is not local control.
Encryption is not sovereignty if the keys are controlled elsewhere.
Compliance is not enough if the wrong jurisdiction can compel access.
Confidential tenants are not a minor detail when public data may be involved.

What Communities Should Ask For

Before approval, communities should ask for:
A data sovereignty assessment.
A public-sector data impact assessment.
An ownership and control map.
A corporate structure map showing parent companies, subsidiaries, operators, tenants, and service providers.
A legal jurisdiction assessment identifying all foreign laws that may apply.
An independent analysis of compelled-access risks.
A data residency and data movement statement.
A cloud architecture and backup-location summary.
An encryption and key-control statement.
A public-sector procurement and privacy impact summary, where applicable.
An Indigenous data sovereignty assessment, where applicable.
A secondary-use and AI-use policy.
A breach, access, and notification plan.
A critical infrastructure dependency assessment.
A public exit and data migration plan for public agencies.
Clear commitments on whether health, education, court, policing, Indigenous, children's, biometric, or other sensitive data may be stored or processed.
Legally enforceable limits on foreign access, secondary use, AI training, cross-border transfer, and undisclosed subcontracting where public or sensitive data is involved.

The Public Interest Standard

No data center should be approved, subsidized, or used for public-sector data until the public understands who controls the data, what laws apply, whether foreign governments can compel access, whether Indigenous and public data sovereignty are respected, and whether local approval creates dependence on foreign digital infrastructure.

A server located here is not the same as data controlled here.

A building can sit inside a community while its legal obligations point somewhere else.

If governments are going to approve the physical infrastructure of the digital world, they must also answer the sovereignty question at the centre of it:

Who has power over the data?

14 - Ownership, Tenants, and Corporate Structure

A data center proposal may appear local on paper.

That does not mean control is local.

A company may incorporate locally, purchase land locally, apply for permits locally, and present itself as a local economic development project while being controlled through parent companies, holding companies, investment funds, real estate trusts, foreign corporations, private equity structures, shell companies, subsidiaries, affiliates, or undisclosed contractual arrangements.

The public should not ask only:

What company name is on the application?

The better question is:

Who ultimately owns, controls, profits from, leases, operates, finances, and carries legal responsibility for the project?

Ownership matters because it determines who receives public benefits, who controls decisions, who has legal obligations, who can sell the project, who can claim subsidies, who can access data, who is responsible for harm, and who remains accountable if something goes wrong.

A data center is not only a building. It may be a real estate asset, a cloud facility, an AI infrastructure site, a leased computing platform, a financial investment, a tax-incentive vehicle, a foreign-controlled subsidiary, or part of a larger corporate strategy.

Communities deserve to know which one they are being asked to approve.

The First Layer Is Not Enough

Looking only at the first level of ownership can be misleading.

A project may be submitted by a numbered company, special-purpose vehicle, local subsidiary, development corporation, landholding company, or newly created entity with little history, few assets, and no meaningful public track record. That entity may be legally responsible on paper while the real financial benefit and decision-making power sit elsewhere.

The land may be owned by one company.

The building may be owned by another.

The servers may be owned by another.

The facility may be operated by another.

The tenants may be undisclosed.

The financing may come from another jurisdiction.

The parent company may be foreign.

The subsidies may flow to one entity while liability rests with another.

This matters because corporate structures can separate profit from responsibility.

A community may think it is negotiating with the company that controls the project, when in fact it is dealing with a thin local layer designed to hold permits, receive incentives, limit liability, or shield the identity of the true beneficiaries.

Public review should therefore require disclosure of beneficial ownership, controlling interests, parent companies, affiliated entities, financing arrangements, major tenants, operators, and entities receiving public support.

A local mailing address is not the same as local accountability.

Beneficial Ownership and Control

Beneficial ownership refers to the people, companies, funds, trusts, investors, or controlling entities that ultimately own or benefit from a project, even if they are not the names listed on the first document.

A data center may be owned through several layers of companies. Some may be incorporated in different provinces, states, countries, or tax jurisdictions. Some may be holding companies. Some may be investment vehicles. Some may exist only to own land, receive leases, isolate risk, or manage tax exposure.

The public should ask for an ownership chart that shows the full chain of control.

That chart should identify the applicant, landowner, building owner, operator, parent companies, investors, lenders, affiliated companies, major tenants, subsidy recipients, and any entity with the power to sell, lease, expand, transfer, mortgage, pledge, or control the project.

Without beneficial ownership disclosure, the public may not know who it is actually dealing with.

Land, Building, Servers, and Operations

A data center can involve several different ownership layers.

The landowner may not be the building owner. The building owner may not be the operator. The operator may not own the servers. The server owner may not control the data. The cloud provider may not be the same entity that received local tax incentives. The company that signs the development agreement may not be the company that profits from the computing services.

Each layer creates different questions.

Who owns the land?
Who owns the building?
Who owns the equipment?
Who operates the facility?
Who leases capacity?
Who controls access?
Who receives revenue?
Who receives public subsidies?
Who signs agreements with the municipality or utility?
Who is responsible for environmental compliance?
Who is liable for contamination, fire, noise, water overuse, grid impacts, data breaches, or abandonment?

The public should not be asked to approve a project without a clear map of these relationships.

Tenants and End Users

A data center may be built for a known tenant, a group of tenants, future tenants, cloud customers, AI companies, government agencies, financial institutions, social media platforms, surveillance companies, cryptocurrency operations, or undisclosed clients.

Tenants matter because they may determine the facility's power demand, water use, cooling needs, data sovereignty risks, security requirements, backup systems, public benefit, and ethical concerns.

An AI training tenant may create different energy and cooling demands than ordinary storage. A government tenant may create public-sector data concerns. A policing, defence, border, intelligence, or surveillance tenant may create civil liberties concerns. A crypto tenant may create different public-interest questions than a hospital cloud service or university research facility.

The public should ask whether the project is being approved for a specific use or for any future tenant the owner can attract.

If tenants are confidential, then the approval should clearly define what categories of use are permitted, what categories are prohibited, what changes require public notice, and what changes require new review.

"Future tenants unknown" should not become a blank cheque.

Subsidies and Who Receives Them

Public subsidies should follow public accountability.

If a data center receives tax incentives, grants, low-interest loans, discounted land, utility discounts, infrastructure support, water access, road upgrades, grid upgrades, or other public benefits, the public should know which entity receives the benefit.

Is the subsidy going to the landowner?

The developer?

The building owner?

The operator?

The tenant?

The parent company?

A real estate trust?

A foreign corporation?

A special-purpose vehicle?

A company that may later sell the asset at a profit?

Subsidy agreements should identify the ultimate beneficiary, not only the local applicant.

The public should also ask whether subsidies transfer if the project is sold. If a company receives public support and then sells the facility to another owner, do the public obligations remain? Are clawbacks triggered? Does the new owner inherit job promises, water limits, reporting duties, community benefits, environmental obligations, and tax commitments?

Public money should not disappear into corporate restructuring.

Liability and Risk

Ownership structure can determine who is responsible when something goes wrong.

If there is a fuel spill, who pays?

If a battery fire contaminates runoff, who pays?

If cooling systems exceed water limits, who pays?

If backup generators violate air standards, who pays?

If noise levels exceed promises, who pays?

If the facility is abandoned, who pays for cleanup?

If public infrastructure was oversized for the project and the company leaves, who pays the debt?

If data is breached or compelled under foreign law, who is accountable?

If the local project company has few assets, can the public recover costs from the parent company?

A company should not be allowed to create a lightly capitalized local entity to receive approvals while shielding the larger corporate group from responsibility.

Public approvals should require parent-company guarantees, performance bonds, environmental bonds, decommissioning funds, insurance, indemnities, and legally enforceable obligations that survive sale, merger, bankruptcy, restructuring, or transfer.

The question is not only who profits if the project succeeds.

The question is who pays if it fails.

Corporate Restructuring and Sale

Data centers can be bought, sold, refinanced, leased, transferred, or bundled into investment portfolios.

A facility approved as a local economic development project may later be sold to a foreign owner, private equity fund, real estate investment trust, cloud provider, infrastructure fund, or unknown buyer. Tenants may change. Operators may change. Parent companies may change. Debt may be refinanced. Public promises may become difficult to enforce if they were tied only to the original applicant.

The public should ask what happens if ownership changes.

Will the municipality, regulator, Indigenous government, utility, or public be notified?

Will approval conditions automatically transfer?

Can the public review a sale to a foreign-controlled entity?

Can subsidies continue after a sale?

Can water licences, grid agreements, land-use approvals, and tax incentives be transferred?

Can the facility be converted to a different use, such as AI training, crypto mining, surveillance infrastructure, or military contracting, without public review?

Approvals should not be written as if ownership will remain unchanged forever.

Financing and Debt

Who finances the project can matter as much as who owns it.

A data center may be financed by banks, pension funds, sovereign wealth funds, private equity firms, infrastructure funds, technology companies, real estate trusts, foreign investors, or public financing. Financing may create control rights, security interests, covenants, step-in rights, or pressure to maximize revenue, expand quickly, reduce costs, or sell the asset.

The public should ask whether lenders or investors have rights that could affect operations, ownership, sale, expansion, or public obligations.

If public subsidies reduce private investment risk, the public should know who benefits.

A project should not be promoted as local development while the financial upside flows mainly to distant investors.

Corporate Track Record

The public should know the track record of the applicant, operator, parent company, major tenants, and controlling entities.

Have they built similar facilities before?

Have they violated environmental laws?

Have they exceeded water limits?

Have they broken tax incentive promises?

Have they been involved in data breaches?

Have they faced labour violations?

Have they abandoned sites?

Have they used complex structures to avoid liability?

Have they received public subsidies elsewhere and failed to deliver promised benefits?

A company's history is not irrelevant.

It is evidence.

Governments should not treat every applicant as trustworthy simply because the current proposal is professionally packaged.

Local Incorporation and Public Messaging

A locally incorporated company may be legitimate.

But local incorporation can also be used to create the appearance of local control.

The public should ask whether the local entity has independent decision-making power, local directors, local employees, local assets, local accountability, and authority to honour public commitments. If every major decision must be approved by a parent company, investor, foreign board, or undisclosed tenant, then the local entity is not the true centre of control.

Public messaging should not be allowed to imply local ownership where only local incorporation exists.

The question is not whether the company has a local registration number.

The question is whether the community has a local accountable party with real authority and real assets.

Core Questions

Ownership Structure

What company is listed as the applicant?

When was it incorporated?

Where was it incorporated?

Who owns the applicant?

Who controls the applicant?

Is the applicant a subsidiary, affiliate, holding company, special-purpose vehicle, numbered company, real estate trust, investment vehicle, or joint venture?

What parent companies sit above it?

Are any parent companies foreign-owned or foreign-controlled?

Who are the beneficial owners?

Will the full ownership chain be disclosed publicly?

Land, Building, and Equipment

Who owns the land?

Who owns the building?

Who owns the servers?

Who owns the cooling systems, backup generators, batteries, substations, and other major equipment?

Who owns the fiber connections?

Who owns any private power generation?

Who owns water, sewer, or cooling infrastructure built for the facility?

Can any of these assets be sold separately?

Can ownership be transferred without public notice or approval?

Foreign Ownership of Land

A data center proposal should disclose not only who operates the facility, but who owns the land beneath it.

Land ownership carries long-term power. It can affect future development, infrastructure rights, water access, utility corridors, resale value, public leverage, security concerns, and community control over strategic sites.

If the land is owned by a foreign corporation, foreign-controlled investment vehicle, foreign state-linked entity, private equity structure, real estate trust, or subsidiary of an overseas parent, the public should know that before approval.

Foreign ownership does not automatically mean a project should be rejected. But it does mean the community should ask additional questions.

Who ultimately owns the land?

Were any laws, bylaws, regulations, ownership limits, disclosure requirements, or review processes related to foreign ownership or control of land waived, exempted, bypassed, reinterpreted, or otherwise avoided in order for this project to proceed?

Can the land be sold without public notice?

Can it be transferred to another foreign owner?

Can land ownership be separated from facility operations?

Can the land be used as collateral?

Can public infrastructure increase the value of foreign-held land?

Can water rights, easements, grid connections, or tax incentives transfer with the land?

Can the public recover benefits if the land is sold after approval?

A community should not discover after infrastructure is built, water access is granted, or zoning is changed that the long-term value of the site has been transferred beyond public reach.

Land is not just a platform for servers.

It is a permanent piece of the community.

Operator and Control

Who will operate the facility?

Is the operator the same as the applicant?

Who controls day-to-day operations?

Who controls security?

Who controls access to the building?

Who controls the servers?

Who controls maintenance?

Who controls environmental compliance?

Who controls emergency decisions?

Who has authority to reduce power use, water use, cooling load, generator testing, noise, lighting, or emissions if impacts occur?

Tenants and Users

Who are the tenants?

Are tenants known or unknown?

Will tenants be disclosed before approval?

What categories of tenants are permitted?

Are AI training, AI inference, cryptocurrency, surveillance, policing, defence, intelligence, government, health, education, court, or public-service tenants possible?

Can tenant use change without public review?

Will future tenants be bound by the same environmental, data sovereignty, public reporting, and community benefit obligations?

If tenants are confidential, how will the public know the facility's real impacts and risks?

Subsidies and Public Benefits

What subsidies, tax incentives, grants, discounted rates, infrastructure supports, land discounts, loans, or public benefits are being requested?

Which entity receives each benefit?

Does the subsidy benefit the applicant, landowner, building owner, operator, tenant, parent company, or investor?

Can subsidies transfer if the project is sold?

Are clawbacks required if job, tax, environmental, water, power, reporting, or community benefit promises are not met?

Will the public know the ultimate beneficiary of public support?

Liability

Who is liable for environmental harm?

Who is liable for water overuse?

Who is liable for air emissions violations?

Who is liable for noise, vibration, or lighting impacts?

Who is liable for fuel spills, battery fires, chemical releases, or contaminated runoff?

Who is liable for public infrastructure costs if the project is delayed, cancelled, sold, or abandoned?

Who is liable for decommissioning and cleanup?

Who is liable for data breaches, foreign compelled access, or misuse of public data?

Does the applicant have enough assets to cover these liabilities?

Will the parent company provide a guarantee?

Sale, Transfer, and Restructuring

Can the project be sold?

Can the land be sold separately from the building?

Can the building be sold separately from the servers?

Can the operator change?

Can tenants change?

Can the project be transferred to a foreign owner?

Can water rights, power agreements, tax incentives, or approvals transfer automatically?

Will the public be notified before ownership changes?

Will public approval be required for major ownership or use changes?

Will all obligations survive sale, merger, restructuring, bankruptcy, or transfer?

Financing and Investors

Who is financing the project?

Are lenders, investors, private equity firms, sovereign wealth funds, pension funds, real estate trusts, or infrastructure funds involved?

Do financiers have control rights?

Can lenders take control if the project defaults?

Could debt obligations pressure the operator to expand, cut costs, increase energy use, or change tenants?

Are public subsidies reducing private financial risk?

Are any municipal, provincial, state, federal, or publicly backed agencies providing loan guarantees, insurance, indemnities, credit support, or other financial risk protections for this project?

Will financing arrangements be disclosed enough for the public to understand control and risk?

Corporate Track Record

Has the applicant built or operated data centers before?

Has the operator?

Has the parent company?

Have any involved companies received public subsidies elsewhere?

Did they meet job, tax, environmental, water, energy, and community benefit promises?

Have they been involved in environmental violations, labour violations, data breaches, litigation, bankruptcy, abandoned projects, or regulatory penalties?

Will governments publish a due diligence report before approval?

Transparency

Will the public receive a corporate structure chart?

Will the public receive a beneficial ownership declaration?

Will major tenants be disclosed?

Will subsidy recipients be disclosed?

Will liability arrangements be disclosed?

Will parent-company guarantees be disclosed?

Will ownership changes be publicly reported?

Will annual ownership and tenant updates be required?

Red Flags

An ownership, tenant, or corporate structure proposal deserves greater scrutiny when the public hears:

"The applicant is locally incorporated."

"Ownership details are commercially sensitive."

"Tenants are confidential."

"Future users have not been finalized."

"The project will be operated by affiliates."

"The company has significant global experience."

"Subsidies are tied to the project, not the parent company."

"Liability is addressed through standard agreements."

"Ownership may change as the project develops."

"Corporate structure is still being finalized."

"Public disclosure could affect competitiveness."

Local incorporation is not local ownership.

A subsidiary is not always the real decision-maker.

A tenant is not irrelevant if its workload determines the public burden.

A subsidy is not transparent if the final beneficiary is hidden.

Liability is not meaningful if the responsible entity has no assets.

What Communities Should Ask For

Before approval, communities should ask for:

A complete corporate structure chart.

A beneficial ownership declaration.

A list of all parent companies, subsidiaries, affiliates, holding companies, special-purpose vehicles, real estate trusts, investment funds, and joint venture partners.

Identification of the landowner, building owner, equipment owner, operator, cloud provider, major tenants, and subsidy recipients.

Disclosure of all foreign ownership or control.

Disclosure of all entities eligible to receive public subsidies, tax incentives, utility discounts, grants, loans, or infrastructure support.

A tenant disclosure statement or permitted-use framework.

A corporate track record and due diligence report.

A financing and investor summary.

A liability map showing responsibility for environmental, financial, operational, emergency, data, and decommissioning risks.

Parent-company guarantees where local entities have limited assets.

Environmental and decommissioning bonds.

Insurance requirements.

Clawback provisions for failed promises.

Public notice requirements for ownership, tenant, operator, or use changes.

Legal conditions ensuring all obligations survive sale, merger, restructuring, bankruptcy, or transfer.

Annual public reporting on ownership, tenants, subsidies, compliance, and liability coverage.

The Public Interest Standard

No data center should be approved, subsidized, or granted access to public infrastructure until the public knows who truly owns it, who controls it, who profits from it, who uses it, who receives public benefits, and who is liable if something goes wrong.

The name on the application is only the beginning of the ownership question.

A community should not be asked to trust a first layer of incorporation when real control may sit behind holding companies, subsidiaries, investment vehicles, foreign parents, confidential tenants, or financial structures designed to separate profit from responsibility.

If the public is expected to provide land-use approval, water, electricity, roads, tax incentives, emergency services, environmental risk, and long-term infrastructure support, then the public has the right to know who is standing on the other side of the agreement.

Accountability requires a name.

Real accountability requires the whole structure behind it.

15 - Cybersecurity and Critical Infrastructure

A data center may be privately owned.

That does not mean its failure would be private.

If a facility hosts government systems, health records, emergency services, financial transactions, utility operations, school platforms, court records, policing systems, communications networks, cloud services, artificial intelligence tools, or other essential digital functions, then it may become part of the public's critical infrastructure.

The public should not ask only:

Is the facility secure?

The better question is:

What happens to the community if this facility fails, is attacked, is breached, is held hostage, is shut down, is sold, is sanctioned, is disconnected, or is compelled to provide access to another authority?

Cybersecurity is not only a technical issue. It is a public safety issue, a governance issue, a sovereignty issue, an emergency planning issue, and a community resilience issue.

A data center can become critical infrastructure without the public ever being told that it has become critical.

That should not happen.

Private Infrastructure, Public Dependence

A data center may begin as a private development project. It may be promoted through jobs, taxes, investment, and innovation. But over time, it may host systems the public depends on.

A municipality may rely on it for records, billing, emergency communications, water systems, traffic controls, public websites, permitting, police dispatch, or council operations. A health authority may rely on it for medical records, diagnostic systems, scheduling, prescriptions, imaging, or patient communication. Schools may rely on it for student records, learning platforms, attendance, testing, and communication with families. Courts may rely on it for filings, evidence, case records, hearings, and legal notices. Utilities may rely on it for grid management, water treatment, billing, monitoring, and outage response.

When private infrastructure becomes essential to public function, the public has the right to know what safeguards exist.

A community should not discover its dependence only after a failure.

Cyberattack and System Failure

Data centers may be targets for cyberattack, ransomware, sabotage, espionage, insider threats, supply-chain attacks, denial-of-service attacks, malware, physical intrusion, remote compromise, or hostile state activity.

They may also fail through ordinary causes: fire, flood, cooling failure, power failure, software error, misconfiguration, equipment failure, human error, construction damage, contractor negligence, or cascading infrastructure failure.

The public should ask whether the facility has been assessed not only for routine security, but for serious failure scenarios.

What happens if systems go offline?

What happens if data is encrypted by ransomware?

What happens if public agencies lose access?

What happens if backups fail?

What happens if cloud services are disrupted?

What happens if emergency services cannot access critical records?

What happens if the facility is physically damaged?

What happens if a cyberattack coincides with wildfire, flood, heat wave, grid failure, or other emergency?

Cybersecurity planning should not assume that crises arrive one at a time.

Critical Public Services

Some data should be treated as especially sensitive because losing access to it can endanger people.

Health systems, emergency response, policing, courts, corrections, utilities, public benefits, child welfare, transportation, water systems, and energy systems are not ordinary customer accounts. They are public lifelines.

If a data center will host or process these systems, the public should ask whether the facility has been designated, regulated, or reviewed as critical infrastructure.

If it has not, why not?

A data center should not receive only a basic land-use review if its failure could disrupt hospitals, emergency dispatch, water treatment, public safety, courts, schools, or government operations.

The level of public review should match the level of public dependence.

Physical Security and Public Impact

Data centers often require significant physical security.

That may include fencing, gates, cameras, guards, access controls, bollards, barriers, surveillance systems, restricted roads, lighting, background checks, vehicle screening, and hardened building design. These measures may be necessary, but they also affect community fit, emergency access, privacy, public space, and local policing demands.

The public should ask whether physical security planning has been coordinated with local emergency services, fire departments, police, utilities, and municipal officials.

A highly secure facility may be difficult for first responders to access during fire, flood, battery incident, chemical release, medical emergency, active threat, or evacuation. Security protocols should not delay emergency response or place responders at unnecessary risk.

The public should also ask whether local policing, fire, emergency medical services, and emergency management agencies will bear new costs because of the facility.

Private security needs should not quietly become public security burdens.

Redundancy, Backups, and Continuity

Data centers are often designed with redundancy.

But redundancy is not the same as resilience.

A facility may have backup power, backup cooling, duplicate network connections, mirrored servers, batteries, generators, and disaster recovery arrangements. The public should know whether those systems protect only the company's operations or whether they protect public services that depend on the facility.

If government or public-service data is hosted there, the public should ask:

Are backups geographically separated?

Are backups protected from ransomware?

Are backups tested?

Can public agencies restore service quickly?

Can systems operate if the data center is offline?

Can services be moved to another provider?

Can data be recovered without permission from a foreign parent company, cloud vendor, or contractor?

A backup that exists only on paper is not a public safety plan.

Supply Chain and Vendor Risk

Cybersecurity does not stop at the building wall.

A data center depends on hardware, software, firmware, cloud platforms, contractors, subcontractors, maintenance providers, security vendors, cooling systems, power systems, battery systems, network equipment, monitoring platforms, remote access tools, and global supply chains.

Each of these may create risk.

The public should ask whether major vendors and subcontractors have been assessed for cybersecurity, foreign control, sanctions exposure, data access, remote administration, supply-chain compromise, and long-term support.

If a facility supports public services or critical infrastructure, governments should know whether any vendor, component, software system, or remote support arrangement creates unacceptable dependence or vulnerability.

A secure building with vulnerable vendors is not secure.

Remote Access and Administrative Control

Many digital systems can be managed remotely.

Remote administration can be efficient, but it can also create cybersecurity and sovereignty risks. If administrators, vendors, cloud providers, or support contractors can access systems from other jurisdictions, the public should know what controls exist.

Who can remotely access the facility's systems?

From where?

Under whose authority?

With what logging?

With what approval?

Can remote access be disabled during emergencies?

Are privileged accounts monitored?

Are subcontractors allowed remote access?

Are foreign-based support teams involved?

The public should not be reassured by the physical location of the facility if operational control can occur elsewhere.

Incident Reporting and Public Notice

When something goes wrong, the public should not be left in the dark.

A data center that supports public services should have clear incident reporting requirements. Cyberattacks, ransomware events, unauthorized access, major outages, backup failures, physical intrusions, fire events, hazardous releases, emergency generator operation, and disruptions to public systems should be reported promptly to the appropriate authorities and, where public services or personal data are affected, to the public.

The public should ask what incidents must be reported, who receives notice, how quickly notice must be given, what information must be disclosed, and whether reports will be public.

Security cannot become a blanket excuse for secrecy.

Some details may need to remain confidential to prevent further harm. But the existence, scale, public impact, and accountability response to major incidents should not be hidden.

Public Costs of Cybersecurity and Emergency Preparedness

If a data center becomes critical infrastructure, public agencies may be expected to support it.

Fire departments may require specialized training. Police may need response plans. Emergency management agencies may need coordination exercises. Utilities may need dedicated protocols. Municipal staff may need cybersecurity planning. Public agencies may need backup communication systems. Regulators may need monitoring capacity.

The public should ask who pays for these costs.

If the facility's private operations require public emergency readiness, the developer should contribute to that readiness. Communities should not be expected to absorb new public safety costs without disclosure, funding, training, and enforceable agreements.

Core Questions

Critical Infrastructure Status

Will the facility host or support critical public services?

Will it support government operations?

Will it support health systems?

Will it support emergency services?

Will it support courts, policing, corrections, utilities, schools, transportation, water systems, energy systems, financial systems, or communications networks?

Has the facility been assessed as critical infrastructure?

If not, why not?

Which agency is responsible for that assessment?

Will critical infrastructure status trigger stronger security, reporting, emergency planning, and public accountability requirements?

Cybersecurity Risk

What cybersecurity risks have been assessed?

Has the facility been assessed for ransomware?

Has it been assessed for sabotage, espionage, insider threats, supply-chain attacks, malware, denial-of-service attacks, misconfiguration, and unauthorized access?

Has an independent cybersecurity audit been completed?

Will audits be repeated?

Will public agencies using the facility receive audit summaries?

Will security standards be legally required or only voluntarily promised?

Public Service Continuity

What public services could be disrupted if the facility fails?

How long could those services be unavailable?

Are backup systems tested?

Are disaster recovery systems tested?

Can public agencies operate if the facility is offline?

Can public data be restored quickly?

Can services be migrated to another provider?

Who decides when public-service systems are restored?

What happens if the operator, cloud provider, or parent company is unavailable, bankrupt, sanctioned, compromised, or legally restrained?

Physical Security

What physical security measures will be used?

Will fencing, cameras, gates, guards, barriers, lighting, surveillance systems, or restricted roads affect the community?

Will security measures interfere with emergency response?

Have local fire, police, emergency medical, and emergency management agencies reviewed the plans?

Will first responders have access during emergencies?

Will private security requirements increase public policing or emergency costs?

Who pays for those costs?

Supply Chain and Vendors

What major hardware, software, network, cooling, power, battery, security, and monitoring vendors are involved?

Are vendors or subcontractors foreign-owned or foreign-controlled?

Can vendors remotely access systems?

Have supply-chain risks been assessed?

Are any components or services subject to foreign legal control, sanctions, export restrictions, or security concerns?

Can critical systems be maintained if a vendor relationship ends?

Remote Access

Who can access systems remotely?

Where are remote administrators located?

Can foreign-based staff access systems?

Can subcontractors access systems?

Are privileged accounts logged and monitored?

Can remote access be disabled during emergencies?

Who approves remote access?

Are public-sector clients told who can access systems that support their services?

Incident Reporting

What incidents must be reported?

Must cyberattacks be reported?

Must ransomware attempts be reported?

Must data breaches be reported?

Must unauthorized access be reported?

Must outages be reported?

Must emergency generator operation be reported?

Must physical intrusions, fires, battery incidents, chemical releases, and major equipment failures be reported?

Who receives notice?

How quickly must notice be given?

Will affected public agencies and individuals be notified?

Will the public receive summaries of major incidents?

Emergency Planning

What happens during a cyberattack?

What happens during a power outage?

What happens during a cooling failure?

What happens during a fire?

What happens during a flood, wildfire, storm, extreme heat, extreme cold, or evacuation?

What happens if a cyberattack occurs during a physical emergency?

Have emergency exercises been conducted?

Are local emergency services trained and funded?

Will emergency plans be updated as the facility expands?

Accountability

Who is liable if a cyberattack disrupts public services?
Who is liable if public data is breached?
Who is liable if emergency systems fail?
Who is liable if a vendor causes the failure?
Who is liable if the operator fails to report an incident?
Are penalties enforceable?
Can public contracts be terminated?
Can permits be reviewed or suspended?
Can public agencies recover costs?
Does the parent company guarantee the obligations of the local operator?

Red Flags

A cybersecurity or critical infrastructure proposal deserves greater scrutiny when the public hears:

"Security details are confidential."
"The facility follows industry standards."
"The data center is privately operated."
"Critical infrastructure status is not part of this land-use review."
"Cybersecurity is handled by the tenant."
"Public-sector use has not been finalized."
"Backups are in place."
"Incidents will be reported as required by law."
"Remote access is controlled through standard procedures."
"Emergency planning will be finalized later."

Security is not accountability.
Confidentiality is not preparedness.
Backups are not resilience unless they are tested.
Private ownership does not erase public dependence.

What Communities Should Ask For

Before approval, communities should ask for:
A critical infrastructure assessment.
A public-service dependency assessment.
An independent cybersecurity risk assessment.
A physical security and emergency access assessment.
A supply-chain and vendor risk assessment.
A remote access and administrative control statement.
A disaster recovery and business continuity plan.
A public-service continuity plan where government or essential services are involved.
An incident reporting and public notification protocol.

A first responder training and funding agreement.

A cybersecurity audit schedule.

A breach, outage, ransomware, and emergency response plan.

A liability and cost-recovery framework.

Parent-company guarantees where local entities have limited assets.

Clear permit-review triggers if security risks, public-service dependencies, ownership, tenants, or uses change.

The Public Interest Standard

No data center should be approved or used for critical public services until the public understands whether it creates public dependence, what happens if it fails, how it will be protected, who can access it, who reports incidents, and who is liable when harm occurs.

A community should not be asked to approve private infrastructure that quietly becomes essential to public life without public scrutiny.

If a data center becomes part of the systems that keep governments operating, hospitals functioning, courts moving, schools connected, utilities running, and emergency services responding, then it is no longer only a private development.

It is part of the public safety landscape.

And the public has the right to know how that landscape is protected.

16 - Privacy, Surveillance, and Public Data

A data center may be described as neutral infrastructure.

But the systems it supports may not be neutral.

If a data center hosts public data, policing systems, immigration records, health systems, school platforms, smart-city tools, facial recognition, predictive analytics, automated decision systems, public-sector artificial intelligence, or surveillance infrastructure, then the public-interest questions change.

The issue is no longer only where the building is located, how much power it uses, how much water it consumes, or who owns it.

The issue becomes what the infrastructure enables.

A data center can store medical records. It can process school data. It can support police databases. It can host court records. It can power smart traffic systems. It can analyze public benefits applications. It can process video feeds. It can support facial recognition. It can train or run AI systems. It can merge datasets that were never meant to be combined. It can make public services faster, but it can also make surveillance deeper, profiling easier, and accountability harder.

The public should not ask only:

Will the data be secure?

The better question is:

What data will be collected, who will use it, what systems will it support, what decisions will it influence, and what safeguards protect the people whose lives are represented inside it?

Public Data Is Not Ordinary Data

Public data is often collected through public power.

People provide information to governments because they need health care, education, permits, benefits, utilities, policing, courts, licences, public housing, emergency services, child services, taxation, transportation, or identification. In many cases, they cannot meaningfully refuse.

That makes public data different from ordinary consumer data.

A person may choose not to use a private app. They cannot easily choose not to appear in a school record, health file, court database, property record, tax file, police report, child welfare file, immigration file, or emergency services system.

Because public data is collected through public authority, it should be governed by public obligations.

A data center that stores, processes, analyzes, or transmits public data should not be treated as merely a private landlord for servers. It becomes part of the machinery through which public power is exercised.

Privacy Is Not Just Security

Security asks whether data is protected from unauthorized access.

Privacy asks a broader question: should the data be collected, used, shared, linked, retained, analyzed, or automated in the first place?

A system can be secure and still be invasive.

A database can be encrypted and still be used to profile people. A smart-city system can be protected from hackers and still track movement through public space. A school platform can be technically secure and still collect excessive data about children. A health system can comply with cybersecurity standards and still expose sensitive information to vendors, analytics tools, or secondary uses. A policing database can be well protected and still enable surveillance, discrimination, or wrongful targeting.

The public should not allow security language to replace privacy scrutiny.

The question is not only whether the data is locked.

The question is whether the data should be there, who has the key, and what the key allows them to do.

Surveillance Infrastructure

Surveillance does not always look like surveillance.

It may appear as traffic management, public safety analytics, smart lighting, school safety software, border management, fraud detection, predictive policing, facial recognition, licence plate readers, public Wi-Fi, emergency response tools, social service analytics, or "efficiency" software.

Each system may be justified separately. Together, they can create a surveillance environment.

A data center may not operate the cameras, sensors, or analytics tools directly, but it may provide the storage, processing power, cloud platform, AI capacity, or integration layer that makes those systems possible.

The public should ask whether the facility will support surveillance tools, public-space monitoring, biometric identification, predictive analytics, policing databases, immigration enforcement, behavioural analysis, or public-sector AI systems.

Infrastructure should not be approved as neutral if its known or likely uses affect civil liberties.

Facial Recognition and Biometric Data

Biometric data deserves special scrutiny.

Faces, fingerprints, iris scans, voiceprints, gait, DNA, and other biometric identifiers are not ordinary data points. They are tied to a person's body. If compromised, misused, or improperly collected, they cannot be easily changed like a password.

Facial recognition systems can raise concerns around consent, accuracy, bias, wrongful identification, public surveillance, chilling effects, protest monitoring, school discipline, policing, immigration enforcement, and the tracking of people in public spaces.

If a data center may store or process biometric data, the public should ask whether that use is allowed, prohibited, limited, audited, or publicly disclosed.

A facility should not become the invisible backend for biometric surveillance without democratic debate.

Policing, Immigration, Courts, and Corrections

Data involving policing, immigration, courts, and corrections can carry serious consequences.

It may affect arrest, detention, bail, sentencing, deportation, parole, probation, risk scoring, investigation, surveillance, child custody, restraining orders, evidence handling, and access to justice.

If a data center hosts or processes this information, the public should ask whether the systems involved are transparent, accountable, challengeable, and protected from misuse.

Will data be used for predictive policing?
Will it be used to score people for risk?
Will it be shared with immigration authorities?
Will it be combined with school, health, housing, social service, or location data?
Will private vendors influence public decisions?
Will affected individuals know when data has shaped a decision about them?

Public-sector data should not be used to create invisible machinery that affects people's rights without their knowledge.

Health, Education, and Children's Data

Health and education data require heightened protection.

Health data can reveal illness, disability, medication, mental health, reproductive care, addiction, trauma, family history, genetics, and vulnerability.

Education data can reveal children's identities, disabilities, behaviour, attendance, learning needs, discipline, family circumstances, language, immigration status, poverty, and mental health concerns.

Children's data is especially sensitive because children cannot meaningfully understand or refuse long-term data collection. Data collected about a child at school may follow them into adulthood if retention, sharing, analytics, or AI use are not strictly limited.

The public should ask whether health, education, and children's data will be stored, processed, analyzed, used for AI, shared with vendors, or combined with other datasets.

A community should not allow children's futures to be converted into permanent data trails because a system was convenient for adults.

Smart Cities and Sensor Networks

Smart-city systems can collect enormous amounts of information.

Traffic sensors, cameras, public Wi-Fi, smart meters, transit cards, parking systems, environmental sensors, licence plate readers, public safety tools, utility systems, building controls, and digital service platforms can all produce data about how people move, gather, consume, travel, work, protest, seek help, or live.

These systems may improve services, but they can also normalize continuous monitoring.

If a data center supports smart-city infrastructure, the public should ask what data is collected, whether it identifies individuals, how long it is retained, who can access it, whether it can be combined with other datasets, whether police or private vendors can use it, and whether residents can opt out.

A city should not become a data extraction system by calling every sensor "smart."

Predictive Analytics and Public-Sector AI

Predictive analytics and AI systems can influence public decisions.

They may be used in policing, child welfare, health triage, education, benefits eligibility, fraud detection, housing, immigration, sentencing, probation, traffic enforcement, emergency response, public finance, and resource allocation.

These tools can reproduce bias, obscure responsibility, and make errors difficult to challenge. They may rely on historical data shaped by inequality, over-policing, under-service, poverty, racism, disability discrimination, gender bias, or institutional neglect.

If a data center supports public-sector AI or predictive analytics, the public should ask whether those systems are disclosed, tested, audited, explainable, appealable, and subject to democratic oversight.

The issue is not only whether the model is accurate.

The issue is whether public power should be exercised through systems the public cannot inspect, understand, or challenge.

Data Linking and Function Creep

Data collected for one purpose can later be used for another.

This is function creep.

A school attendance system may become a policing tool. A public benefits database may become a fraud-detection system. A traffic camera network may become a protest monitoring system. Health data may become an insurance, employment, or risk prediction tool. Smart-city sensors may become immigration enforcement infrastructure. Public Wi-Fi data may become movement tracking.

The public should ask whether data hosted in the facility can be linked, repurposed, sold, shared, analyzed, or used for purposes beyond the original reason it was collected.

The more datasets a data center can store and process, the more important it becomes to prevent invisible expansion of use.

Consent given for one public service should not become consent for everything a future government, vendor, or algorithm might want to do.

Vendor Power and Democratic Oversight

Public agencies may rely on private vendors for software, storage, analytics, AI systems, security, and cloud services.

That can shift power away from public institutions and toward private companies. Vendors may control system design, data access, analytics tools, proprietary models, contract terms, audit logs, technical documentation, pricing, upgrades, and the ability to leave the platform.

The public should ask whether governments remain in control or whether vendors become the real decision-makers.

Can the government audit the system?

Can it explain decisions made through the system?

Can it leave the vendor?

Can it delete data?

Can it prevent secondary use?
Can it inspect algorithms?
Can it publish impact assessments?
Can affected people appeal decisions?
A public agency should not outsource accountability along with the data.

Consent, Notice, and Choice

People should know when their data is being collected, stored, analyzed, shared, or used to make decisions about them.

In public systems, consent is often limited because people need the service. That makes notice, minimization, legal limits, purpose restrictions, access rights, correction rights, appeal rights, and deletion rules even more important.

If a data center hosts public data, the public should ask whether individuals are told:
What data is collected.
Why it is collected.
Where it is stored.
Who has access.
How long it is kept.
Whether it is shared.
Whether it is used for AI or analytics.
Whether it affects decisions.
How they can see, correct, challenge, or delete it.

A person should not have to become a privacy expert to understand how public systems use their life.

Retention, Deletion, and the Right to Be Forgotten

Data should not be kept forever just because storage is cheap.

Long retention periods increase the risk of breach, misuse, surveillance, profiling, secondary use, and harm. Public data should have clear retention limits based on necessity, law, rights, public accountability, and individual protection.

The public should ask how long each category of data will be kept, when it will be deleted, who verifies deletion, whether backups are also deleted, and whether archived data can be searched, analyzed, or used for AI.

A system that never forgets can become a system that never forgives.

Transparency and Public Registers

If public data or surveillance tools are involved, secrecy should be limited.

Communities should ask for public registers of major public-sector datasets, surveillance technologies, AI systems, biometric systems, smart-city sensors, data-sharing agreements, vendor contracts, retention schedules, and impact assessments.

Not every security detail needs to be public. But the existence and purpose of systems that affect public rights should be visible.

People cannot debate what they are not allowed to know exists.

Core Questions

Public Data

Will the facility store, process, transmit, back up, mirror, analyze, or host public-sector data?

Which public agencies will use the facility?

Will it involve municipal, provincial, state, federal, Indigenous, health, education, court, policing, immigration, corrections, utility, transportation, or social service data?

Will public data be separated from commercial data?

Will public data be used for analytics, AI, model training, profiling, or secondary purposes?

Will public agencies publish privacy impact assessments before using the facility?

Personal and Sensitive Data

Will the facility handle personal information?

Will it handle health data?

Will it handle children's data?

Will it handle education records?

Will it handle biometric data?

Will it handle geolocation data?

Will it handle financial data?

Will it handle social service, housing, disability, addiction, mental health, family violence, immigration, or legal data?

What heightened safeguards apply to sensitive data?

Surveillance Uses

Will the facility support surveillance tools?

Will it support facial recognition?

Will it support licence plate readers?

Will it support public camera networks?

Will it support smart-city sensors?

Will it support predictive policing?

Will it support immigration enforcement?

Will it support protest monitoring, crowd analysis, or public-space tracking?

Will it support social media monitoring or open-source intelligence tools?

Are any surveillance uses prohibited?

Facial Recognition and Biometrics

Will biometric data be stored or processed?

What types of biometric data?

Who collects it?

Was consent obtained?

Can people refuse?

What accuracy standards apply?
Have bias and error rates been assessed?
Can people challenge a match?
Are law enforcement or immigration agencies allowed access?
Will biometric data be deleted when no longer needed?
Are biometric uses publicly disclosed?

Public-Sector AI and Predictive Analytics

Will the facility support AI systems used by government or public agencies?
Will AI systems affect benefits, policing, courts, corrections, health care, education, immigration, housing, transportation, utilities, or emergency services?
Will algorithms be disclosed?
Will impact assessments be public?
Will systems be audited for bias, accuracy, safety, and rights impacts?
Will individuals know when AI affected a decision?
Can decisions be appealed to a human?
Can agencies explain how decisions were made?
Are any AI uses prohibited?

Data Linking and Secondary Use

Can data from different public systems be linked?
Can data be shared between agencies?
Can data be shared with police, immigration, private vendors, researchers, advertisers, insurers, employers, or third parties?
Can data collected for one purpose be reused for another?
Can metadata be used?
Can de-identified data be re-identified?
Can data be used to train AI systems?
Who approves secondary use?
Will the public be notified?

Vendor Control

What vendors are involved?
Can vendors access public data?
Can vendors use data for product improvement, analytics, AI training, or commercial purposes?
Are vendors prohibited from selling or sharing data?
Can governments audit vendor systems?
Can governments inspect algorithms or models?
Can governments leave the vendor without losing access to data or services?
Can public data be returned and deleted?
Are vendor contracts public?

Consent, Notice, and Rights

Are individuals told where their data is stored?
Are they told who can access it?
Are they told whether it may be used for AI or analytics?
Can they access their data?
Can they correct their data?
Can they challenge decisions made with their data?
Can they request deletion where legally appropriate?
Can they opt out where possible?
What protections exist when consent is not meaningful because the service is essential?

Retention and Deletion

How long will each category of data be retained?
Who sets the retention period?
Are backups subject to deletion rules?
Are logs and metadata subject to deletion rules?
Can archived data be searched or analyzed?
Is data deleted automatically when no longer needed?
Who verifies deletion?
Are deletion failures reported?

Transparency and Oversight

Will there be a public register of public-sector datasets hosted or processed?
Will there be a public register of surveillance technologies?
Will there be a public register of AI systems used by public agencies?
Will privacy impact assessments be public?
Will data-sharing agreements be public?
Will surveillance and AI tools require council, legislative, or public approval?
Will an independent privacy commissioner, auditor, ethics body, or oversight office review the systems?
Will affected communities be consulted before high-risk systems are used?

Harm and Remedies

What happens if data is misused?
What happens if surveillance tools are abused?
What happens if AI makes a harmful decision?
What happens if biometric identification is wrong?
What happens if public data is shared improperly?
What happens if a vendor violates restrictions?
Can affected people seek remedies?
Can contracts be terminated?
Can systems be suspended?

Can public agencies be required to stop using harmful tools?

Red Flags

A privacy, surveillance, or public data proposal deserves greater scrutiny when the public hears:
"The facility is only infrastructure."
"Privacy is handled by the tenant."
"The data will be secure."
"The system complies with privacy law."
"AI use depends on customer needs."
"Surveillance tools are not part of this application."
"Public-sector use has not been finalized."
"Data may be used to improve services."
"Data is de-identified."
"Facial recognition will only be used for safety."
"Predictive analytics will improve efficiency."
"Vendor contracts are confidential."

Infrastructure is not neutral when it enables surveillance.
Security is not privacy.
De-identification is not always protection.
Efficiency is not consent.
A public service should not become a data trap.

What Communities Should Ask For

Before approval or public-sector use, communities should ask for:
A public data impact assessment.
A privacy impact assessment.
A surveillance impact assessment.
A biometric and facial recognition assessment, where applicable.
A public-sector AI and automated decision-system assessment.
A data-linking and secondary-use policy.
A public register of datasets, surveillance tools, and AI systems.
A vendor access and data-use policy.
A data retention and deletion schedule.
A consent, notice, access, correction, appeal, and remedy framework.
An Indigenous data governance assessment where Indigenous data may be involved.
A children's data protection assessment where education or youth data may be involved.
A health data protection assessment where medical data may be involved.
A policing, courts, corrections, or immigration data assessment where justice-related data may be involved.
A public oversight and audit plan.

Clear prohibitions on unauthorized AI training, biometric surveillance, secondary use, data sale, and undisclosed data sharing.

Legally enforceable penalties, contract termination rights, system suspension powers, and public remedies if privacy or surveillance safeguards are violated.

The Public Interest Standard

No data center should be approved, subsidized, or used for public-sector systems until the public understands whether it will support surveillance, biometric identification, predictive analytics, public-sector AI, smart-city monitoring, or the storage and processing of sensitive public data.

A community should not be told that privacy is someone else's problem because the building is only "infrastructure."

Infrastructure is how power becomes permanent.

If a data center becomes the place where public records, surveillance systems, AI tools, school platforms, health files, policing data, court records, immigration systems, and smart-city sensors are stored or processed, then the public has the right to ask what kind of society that infrastructure is helping to build.

The question is not only whether the data is safe.

The question is whether the people are.

Part Four: Economics and Public Risk

17 - Jobs and Economic Claims

Data center proposals often arrive with large numbers.

Investment value.

Construction spending.

Projected tax revenue.

Regional economic impact.

Innovation language.

Job creation claims.

Technology-sector branding.

Promises of growth.

These numbers can be persuasive, especially for communities facing budget pressure, job losses, population change, infrastructure needs, or economic uncertainty. A data center may be presented as a rare opportunity: a chance to attract investment, modernize the local economy, expand the tax base, and become part of the digital future.

Those claims deserve careful examination.

The public should not ask only:

How many jobs will the project create?

The better question is:

What kind of jobs, for whom, for how long, at what public cost, with what guarantees, and compared to what alternatives?

A data center may involve billions of dollars in capital investment while creating relatively few permanent local jobs. It may generate significant construction work, but much of that labour may be temporary, specialized, imported, subcontracted, or unavailable to local workers. It may promise tax revenue while also seeking tax exemptions, discounted power, public infrastructure, water access,

road upgrades, or other subsidies. It may describe itself as transformative while providing limited long-term employment once construction ends.

Economic development should not be accepted as a slogan.

It should be tested as a public-interest claim.

Construction Jobs Are Not Permanent Jobs

Many data center job claims rely heavily on construction employment.

Construction jobs matter. They can provide wages, contracts, training, and local economic activity. But construction jobs are not the same as permanent jobs. They are temporary by design. Once the facility is built, the number of ongoing jobs may fall sharply.

The public should ask every proposal to separate:

Construction jobs.

Permanent operational jobs.

Direct jobs.

Indirect jobs.

Induced jobs.

Local jobs.

Non-local jobs.

Full-time jobs.

Part-time jobs.

Contract jobs.

Union jobs.

Temporary jobs.

Specialized imported jobs.

Job claims should not be bundled together in a way that makes a short construction period look like long-term employment.

If a project claims thousands of jobs, the public should ask how many will exist five years after opening.

Permanent Jobs and Automation

Data centers can be highly automated.

A large facility may require relatively few permanent staff compared with its land use, power demand, water demand, tax incentives, and infrastructure burden. Ongoing work may include security, maintenance, electrical systems, cooling systems, network operations, cleaning, landscaping, management, monitoring, and technical support. Some of those jobs may be on site. Others may be remote, contracted, rotational, or centralized elsewhere.

The public should ask how many permanent jobs will be physically located in the community.

It should also ask what kinds of jobs they are. Are they high-wage technical positions? Security positions? Maintenance jobs? Contracted cleaning jobs? Remote monitoring roles? Jobs requiring specialized credentials local workers do not have? Jobs controlled by vendors rather than the facility owner?

A facility should not be allowed to imply broad local employment when the long-term staffing model is small, remote, outsourced, or automated.

Local Hiring

A job is not a local benefit unless local people can realistically get it.

The public should ask whether the developer has committed to local hiring, local training, apprenticeships, union labour, fair wages, Indigenous employment, youth training, partnerships with colleges or trade schools, and pathways for workers already living in the region.

A project should disclose what percentage of construction and permanent jobs are expected to go to local workers.

If specialized labour will be brought in from outside the community, that should be stated plainly. If permanent jobs require credentials not available locally, the project should include a training plan before approval, not after the ribbon-cutting.

Local hiring should not be aspirational language. It should be measurable, enforceable, and publicly reported.

Job Quality

Not all jobs are equal.

The public should ask whether jobs created by the project will provide living wages, benefits, stable hours, safe working conditions, training, advancement, union access, local hiring, and long-term security.

A project should not be praised for creating jobs if many of those jobs are temporary, low-wage, subcontracted, precarious, or unavailable to local residents.

Job quality should be part of the economic assessment.

If public land, tax incentives, discounted utilities, infrastructure support, or other subsidies are involved, the public has the right to demand that jobs meet a public-benefit standard.

Public Cost Per Job

One of the most important questions is simple:

How much public money is being spent per permanent local job?

If a data center receives tax exemptions, discounted land, infrastructure upgrades, grants, low-interest loans, water access, discounted electricity, road upgrades, sewer capacity, grid upgrades, or other public benefits, those costs should be compared to the number of permanent local jobs created.

A project may sound impressive when described as a billion-dollar investment. It may look different if the public cost per permanent job is extremely high.

The public should ask for a transparent cost-per-job calculation that includes all public supports, not only direct grants.

That calculation should distinguish between construction jobs and permanent jobs. It should not use temporary construction employment to justify long-term subsidies unless the subsidy is also temporary and proportionate.

Tax Revenue Claims

Data centers may be promoted as sources of tax revenue.

But tax revenue claims should be examined carefully.

Will the project pay full property taxes?

Will it receive tax abatements, exemptions, holidays, freezes, rebates, or special assessments?

Will equipment be taxed?

Will servers be taxed?

Will land value be reassessed?

Will the facility be depreciated in ways that reduce revenue?

Will future councils be bound by long-term tax deals?

Will tax revenue exceed the public costs of roads, water, sewer, emergency services, grid upgrades, policing, fire protection, administration, and environmental monitoring?

A tax revenue promise is not meaningful unless it is net of public cost.

The public should ask for the projected gross revenue, net revenue, timeline, assumptions, exemptions, clawbacks, and risks.

Local Business Benefits

A data center may create opportunities for local businesses, but those benefits should not be assumed.

Construction may involve contractors, suppliers, hotels, restaurants, fuel providers, electricians, equipment rental, trucking, and other services. Operations may require maintenance, security, cleaning, landscaping, snow removal, food services, waste handling, and specialized services.

The public should ask whether local businesses are eligible and prepared to benefit.

Will procurement favour local suppliers?

Will contracts be broken into sizes local firms can bid on?

Will Indigenous businesses be included?

Will small businesses have access to opportunities?

Will procurement data be reported publicly?

Will the project rely mostly on national or international vendors?

A local economic impact claim should identify who actually receives the spending.

Opportunity Cost

Land, water, electricity, tax capacity, public attention, staff time, infrastructure funding, and political energy are limited.

Approving a data center may mean not approving something else. It may use land that could support housing, agriculture, conservation, public services, small business growth, recreation, manufacturing, food systems, renewable energy, or community infrastructure. It may reserve grid capacity that other users need. It may consume water capacity that could support future housing or farms. It may use public subsidies that could fund other priorities.

The public should ask what alternatives were considered.

What else could the land be used for?
What else could the water support?
What else could the electricity power?
What else could public subsidies fund?
What other economic development options would create more jobs, more local ownership, more public value, or less environmental burden?
Economic development is not only about saying yes to investment.
It is about choosing the kind of development that best serves the community.

Displacement and Housing Pressure

Large construction projects can affect local housing and services.

If hundreds or thousands of temporary workers arrive during construction, the community may experience pressure on rental housing, hotels, roads, health services, restaurants, emergency services, policing, and public amenities. In smaller communities, temporary workforce demand can affect affordability and availability for local residents.

The public should ask whether the project includes a workforce housing plan.
Will temporary workers be housed locally?
Will rents rise?
Will hotels be occupied for long periods?
Will the project affect housing for residents, students, seniors, low-income workers, or seasonal workers?
Will public services face increased demand?
Will the developer contribute to mitigation?

Construction employment can benefit a community, but only if the community is prepared for the pressures that come with it.

Labour Conditions and Worker Safety

Data center construction and operation can involve electrical hazards, heavy equipment, heat, confined spaces, high-voltage systems, fuel storage, battery systems, fire suppression systems, cooling chemicals, working at heights, and security-controlled environments.

The public should ask what labour standards will apply.
Will workers have safe conditions?
Will contractors be vetted?
Will there be union access?
Will wage theft, misclassification, unsafe subcontracting, or labour exploitation be prevented?
Will temporary workers have proper housing, transportation, health access, and legal protection?
Will workplace injuries and safety violations be reported?
Publicly supported projects should meet high labour standards.

Promises Must Be Enforceable

Economic claims should become enforceable obligations if they are used to justify approval or subsidy.

If the developer claims a certain number of permanent jobs, local hiring, tax revenue, community benefits, training programs, Indigenous procurement, or local business spending, those claims should be written into legally binding agreements.

The public should ask what happens if the promises are not met.

Are subsidies clawed back?

Are tax benefits reduced?

Are penalties imposed?

Are public reports required?

Can future phases be delayed?

Can permits be reviewed?

Can community benefit agreements be enforced?

A promise made at a podium should not disappear after approval.

Core Questions

Job Numbers

How many construction jobs will be created?

How many permanent operational jobs will be created?

How many jobs will be full-time?

How many will be part-time?

How many will be temporary?

How many will be contract positions?

How many will be remote?

How many will be physically located in the community?

How many jobs will exist five years after opening?

Are job figures direct, indirect, induced, or combined?

Are job estimates independently verified?

Local Hiring

What percentage of construction jobs will go to local workers?

What percentage of permanent jobs will go to local workers?

Will local hiring commitments be legally binding?

Will Indigenous hiring commitments be included?

Will apprenticeships be created?

Will training programs be funded?

Will partnerships be created with local colleges, trade schools, unions, Indigenous governments, or workforce agencies?

Will hiring data be publicly reported?

Job Quality

What wages will be paid?

Will jobs provide benefits?

Will jobs provide stable hours?

Will jobs provide training and advancement?
Will union labour be used?
Will contractors meet labour standards?
Will subcontractors be disclosed?
Will workplace safety requirements be strengthened?
Will workers have protections from misclassification, wage theft, unsafe housing, or exploitation?

Public Cost Per Job

What public subsidies are being provided?
What tax incentives are being provided?
What infrastructure costs are being covered by the public?
What discounted utility rates are being offered?
What grants, loans, land discounts, or public supports are involved?
What is the total public cost?
What is the public cost per construction job?
What is the public cost per permanent local job?
What is the public cost per full-time equivalent job?
Are these figures public before approval?

Tax Revenue

What gross tax revenue is projected?
What net tax revenue is projected after public costs?
Will the project receive tax exemptions, abatements, freezes, rebates, or special assessments?
How long will tax incentives last?
Will servers, equipment, buildings, and land be taxed?
Will depreciation reduce revenue?
Will future councils be bound by current tax deals?
What happens if tax revenue is lower than projected?
Are clawbacks included?

Local Business and Procurement

What local procurement commitments exist?
Will local businesses be able to bid on construction contracts?
Will local businesses be able to bid on operational contracts?
Will Indigenous businesses be included?
Will small businesses be included?
Will procurement be public?
Will spending actually remain in the community?
Will the project rely mainly on outside vendors?

Opportunity Cost

What alternative uses for the land were considered?

What alternative uses for the water were considered?
What alternative uses for the electricity were considered?
What alternative uses for public subsidies were considered?
Could another development create more permanent local jobs?
Could another development create more public value with less environmental burden?
Will the data center limit housing, farming, conservation, renewable energy, small business, or public-service development?

Housing and Community Services

Will construction create temporary housing demand?
How many temporary workers will be present at peak construction?
Where will they live?
Will local rents or hotel availability be affected?
Will health services, emergency services, policing, roads, restaurants, or public amenities face pressure?
Will the developer fund mitigation?
Will a workforce housing plan be required?

Enforcement

Which economic promises are legally binding?
Which promises are only promotional?
What reporting is required?
How often will job numbers be reported?
Who verifies job numbers?
Are subsidies clawed back if job promises are not met?
Are tax benefits reduced if public benefits are not delivered?
Can future phases be delayed if commitments are not met?
Can the public see compliance reports?

Red Flags

A jobs or economic claims proposal deserves greater scrutiny when the public hears:
"The project will create thousands of jobs."
"The investment will transform the region."
"The facility will attract innovation."
"Economic impacts will be significant."
"Construction jobs and permanent jobs are reported together."
"Local hiring will be encouraged."
"Jobs will depend on future tenants."
"Tax revenue will increase over time."
"Incentives are needed to remain competitive."
"Public costs will be offset by growth."
"Workforce details will be finalized later."

Investment is not the same as local benefit.

Construction work is not the same as permanent employment.

Economic impact is not the same as public value.

A tax promise is not meaningful without the cost side of the ledger.

What Communities Should Ask For

Before approval, communities should ask for:

A full economic impact assessment.

Separate construction and permanent job estimates.

A local hiring plan.

An Indigenous hiring and procurement plan where appropriate.

A job quality and wage assessment.

A workforce training and apprenticeship plan.

A public cost-per-job calculation.

A full subsidy and tax incentive disclosure.

A gross and net tax revenue projection.

A local procurement plan.

A workforce housing and community services impact assessment.

An opportunity cost analysis.

A public reporting plan for jobs, wages, procurement, taxes, and subsidies.

Independent verification of economic claims.

Legally enforceable job, wage, local hiring, procurement, tax, and community benefit commitments.

Clawbacks, penalties, and permit-review triggers if promises are not met.

The Public Interest Standard

No data center should be approved or subsidized based on economic claims until the public knows how many permanent local jobs will actually exist, what those jobs will pay, who can access them, what the public will spend to create them, and whether the promised benefits are legally enforceable.

A community should not be asked to trade land, water, electricity, infrastructure, tax capacity, and environmental risk for vague promises of growth.

Jobs matter.

But so do the quality of those jobs, the cost of those jobs, the durability of those jobs, and the honesty of the claims used to sell them.

Economic development is not proven by the size of the announcement.

It is proven by what remains for the community after the announcement is over.

18 - Tax Incentives and Public Subsidies

A data center may be presented as private investment.

That does not mean it is privately paid for.

Data center proposals often involve public support: property tax breaks, sales tax exemptions, discounted electricity, discounted water, road upgrades, transmission upgrades, sewer expansion, grants, low-interest loans, land discounts, infrastructure funding, workforce subsidies, regulatory fast-tracking, or public assumption of risk.

Some of these supports may be obvious. Others may be hidden inside utility rates, infrastructure budgets, tax agreements, economic development programs, land-use changes, or long-term service commitments.

The public should not ask only:

How much private money is the company investing?

The better question is:

How much public value is being given up, who receives it, what the public gets in return, and what happens if the promises are not kept?

A subsidy is not always a cheque. A subsidy can be a tax that is not collected, a road built for one user, a water rate below true cost, a grid upgrade paid by ratepayers, land sold below market value, public staff time devoted to private development, or a long-term agreement that limits future public choices.

If a data center requires public support, the public has the right to see the full price tag.

Subsidies Should Be Named

Public support should be named clearly.

Too often, subsidies are described as "incentives," "partnerships," "economic development tools," "competitiveness measures," "rate structures," "servicing agreements," or "strategic investments." Those phrases may sound neutral, but they can conceal the transfer of public value to private entities.

A property tax exemption is a subsidy.

A sales tax exemption is a subsidy.

A discounted power rate is a subsidy.

A discounted water rate is a subsidy.

A publicly funded road upgrade is a subsidy if it primarily serves the project.

A transmission upgrade paid through general rates is a subsidy if it primarily enables private load growth.

A grant is a subsidy.

A low-interest public loan is a subsidy.

Public land sold below market value is a subsidy.

A public agency absorbing environmental monitoring, emergency planning, or administrative costs is a subsidy.

The first act of accountability is naming what the public is providing.

The Full Public Cost

A subsidy should not be measured only by the amount written in a press release.

The full public cost includes direct and indirect support. It includes money spent, revenue forgone, infrastructure built, services expanded, risks assumed, and future obligations created.

A data center may receive no direct grant and still be heavily subsidized through roads, water infrastructure, sewer capacity, grid upgrades, tax abatements, discounted electricity, discounted water, staff time, land-use changes, and emergency service demands.

The public should ask for a complete subsidy ledger before approval.

That ledger should identify every public contribution from every level of government and every public or regulated utility. It should include municipal, provincial, state, federal, utility, water authority, economic development agency, infrastructure fund, and public-finance contributions.

A project should not be allowed to appear unsubsidized because the public cost is scattered across different budgets.

Tax Breaks and Forgone Revenue

Tax incentives are often treated as painless because they are framed as future revenue the public would not otherwise receive.

That framing is incomplete.

When a government grants a tax break, it gives up public revenue that could otherwise support roads, schools, emergency services, libraries, water systems, housing, public health, climate adaptation, or debt reduction. If the project requires services and infrastructure while paying reduced taxes, existing residents and businesses may carry a larger share of the public burden.

The public should ask:

What taxes would the project pay without incentives?

What taxes will it actually pay?

How long will the discount last?

What services will the facility require during the discount period?

Will the tax break outlast the construction jobs?

Will future councils be bound by the agreement?

Will the public ever recover the forgone revenue?

A tax incentive is not free because it is invisible on the spending side of the budget.

Discounted Electricity and Water

Discounted electricity and water deserve special scrutiny.

Electricity and water are not ordinary commodities. They are shared systems with public consequences. If a data center receives discounted rates, special tariffs, industrial pricing, interruptible arrangements, or privately negotiated agreements, the public should know whether other users are affected.

A discounted rate may shift costs to households, farms, small businesses, schools, hospitals, municipalities, or future ratepayers. It may reduce utility revenue needed for maintenance. It may

encourage overconsumption. It may create unequal access to public resources. It may reserve capacity for a private user while other public needs wait.

The public should ask whether the data center is paying the full cost of the electricity and water it uses, including generation, transmission, distribution, treatment, delivery, maintenance, drought planning, emergency capacity, infrastructure expansion, and environmental impacts.

A low rate is not a public benefit if the public pays the difference elsewhere.

Infrastructure Subsidies

Infrastructure subsidies can be the largest and least visible form of public support.

A data center may require roads, bridges, intersections, water lines, sewer systems, stormwater systems, substations, transmission lines, distribution upgrades, fiber routes, emergency access, fuel routes, or public safety improvements. These may be described as general infrastructure, regional development, or future growth capacity.

But the public should ask who really needs the upgrade and who really benefits.

If infrastructure is built because the data center requires it, the cost should not quietly fall on taxpayers or ratepayers. If infrastructure is oversized for future data center expansion, industrial clustering, or speculative development, the public should know that before paying for it.

Infrastructure support should be disclosed project by project and system by system.

The public should not be asked to fund the skeleton of a private industrial corridor while being told it is simply routine servicing.

Grants, Loans, and Financial Support

Direct public financial support should be transparent.

Grants, low-interest loans, loan guarantees, tax credits, workforce funding, site-preparation funding, research incentives, clean-energy incentives, export support, and infrastructure programs may all reduce private risk.

The public should ask why support is needed.

Would the project proceed without it?

Is the company financially viable?

Is the public receiving ownership, revenue sharing, equity, enforceable benefits, or only promises?

Are public funds supporting a local public benefit or increasing the profit margin of a private owner?

Are grants or loans going to a local entity, a parent company, a developer, a tenant, a utility, or an investor?

If public money reduces private risk, the public should receive enforceable public returns.

Subsidies Across Multiple Levels of Government

A company may receive support from several levels of government at once.

A municipality may offer tax reductions. A province or state may offer grants, training funds, power arrangements, water access, or infrastructure support. A federal government may offer tax

credits, loans, clean-energy incentives, or strategic industry funding. A utility may offer special rates or cost-sharing. A regional authority may fund roads, water, or sewer expansion.

Each government may evaluate only its own contribution.

The public should see the combined total.

A project that looks reasonable at one level of government may look much less reasonable when all public supports are added together.

No subsidy should be approved in isolation if the project depends on a stack of public benefits.

Who Receives the Benefit?

Subsidies should not be attached only to a project name.

The public should know which entity receives each benefit.

Does the subsidy go to the landowner?

The developer?

The building owner?

The operator?

The tenant?

The cloud provider?

The parent company?

A real estate investment trust?

A private equity fund?

A foreign-controlled corporation?

A special-purpose vehicle that may later sell the asset?

This matters because public benefits can increase private asset value. A tax break, road upgrade, grid connection, water agreement, or rezoning decision may make the land or facility more valuable. The original recipient may then sell the project, capturing the public-created value while long-term obligations remain with the community.

The public should ask whether subsidies transfer on sale, whether clawbacks apply, and whether public obligations follow the asset.

Clawbacks and Conditions

No public subsidy should be granted without enforceable conditions.

If the company promises jobs, local hiring, tax revenue, water efficiency, renewable energy, public reporting, community benefits, waste heat recovery, environmental performance, data sovereignty protections, or local procurement, those promises should be written into binding agreements.

Clawbacks should apply if promises are not met.

That means public benefits can be reduced, recovered, suspended, or cancelled if the company fails to deliver. Clawbacks should apply to job shortfalls, wage failures, missed local hiring targets, environmental violations, water overuse, power demand changes, undeclared tenant changes, sale of the project, abandonment, bankruptcy, or failure to report required information.

A subsidy without a clawback is a gift.

A public-interest agreement requires consequences.

Time Limits and Review Points

Subsidies should not run indefinitely.

A tax break or discounted rate may be justified for a short start-up period in some circumstances. That does not mean the public should subsidize a mature facility for decades.

The public should ask how long each subsidy lasts, when it is reviewed, whether it declines over time, whether it can be renewed, and whether renewal requires public approval.

Long-term subsidies are especially risky because conditions change. Technology changes. Ownership changes. Tenants change. Water conditions change. Grid conditions change. Public budgets change. Community needs change.

No council or government should casually bind future residents to decades of public support without periodic review.

Public Transparency

Subsidy agreements should be public.

Some narrow commercial details may require protection, but the public should be able to see the value of the subsidy, the recipient, the term, the conditions, the public obligations, the clawbacks, the reporting requirements, the enforcement mechanism, and the projected public return.

Confidentiality should not be used to hide public cost.

If a company wants public support, it should accept public scrutiny.

Public Return on Public Investment

The public should receive a measurable return for any public subsidy.

That return may include permanent local jobs, tax revenue, local procurement, workforce training, Indigenous employment, community benefit agreements, public broadband, waste heat for public facilities, water restoration, grid improvements that serve residents, environmental monitoring, emergency service funding, or other enforceable benefits.

The return should be measured against the full public cost.

A subsidy should not be justified by vague claims of growth, innovation, competitiveness, or regional branding. Those may be benefits, but they are not substitutes for measurable public value.

The central question is:

Would the public receive more benefit by using the same money, land, water, electricity, or infrastructure capacity for something else?

Core Questions

Subsidy Identification

What public subsidies are being requested?

What tax incentives are being requested?

What grants are being requested?

What loans or loan guarantees are being requested?

What discounted utility rates are being requested?

What infrastructure support is being requested?

What public land, easements, permits, water rights, or grid capacity are being provided?

Are any subsidies indirect, hidden, delayed, or provided through utilities or infrastructure programs?

Full Public Cost

What is the total public cost of the project?

What revenue will be forgone?

What infrastructure will be publicly funded?

What utility costs will be shifted to ratepayers?

What administrative, monitoring, emergency service, legal, and regulatory costs will public bodies carry?

What costs will be borne by municipal taxpayers?

What costs will be borne by provincial, state, or federal taxpayers?

What costs will be borne by utility customers?

Has a full subsidy ledger been published?

Tax Incentives

Will the project receive property tax breaks?

Will it receive sales tax exemptions?

Will it receive equipment tax exemptions?

Will servers or computing equipment be taxed?

Will land, buildings, machinery, and equipment be assessed at full value?

Will the project receive tax freezes, abatements, rebates, holidays, special assessments, or payment-in-lieu agreements?

How long will each tax incentive last?

What would the project pay without incentives?

What will it actually pay?

What public services will it use while receiving tax reductions?

Electricity and Water Discounts

Will the project receive discounted electricity?

Will it receive a special tariff?

Will it receive discounted transmission or distribution charges?

Will it receive discounted water?

Will it receive special wastewater or sewer rates?

Will other users pay more because of these discounts?

Will rates reflect the full cost of service, infrastructure, maintenance, emergency capacity, and environmental impact?

Will the public see the rate agreements?

Can rates be changed if project demand exceeds projections?

Infrastructure

What roads, bridges, intersections, water systems, sewer systems, stormwater systems, transmission lines, substations, transformers, distribution upgrades, pipelines, fiber routes, emergency access, or public facilities are required?

Who pays for each upgrade?

Are upgrades sized for the current project or future expansion?

Will infrastructure built for the project primarily serve the public or the data center?

Will costs be recovered from the developer?

Will maintenance costs fall to the public?

Will public infrastructure increase the private value of the land or facility?

Recipients and Beneficiaries

Which entity receives each subsidy?

Is the recipient the applicant, landowner, developer, building owner, operator, tenant, parent company, investor, or utility?

Who ultimately benefits from the public support?

Will beneficial ownership be disclosed?

Can subsidies transfer if the project is sold?

Will public obligations transfer with the subsidy?

Can the company sell the publicly supported asset and keep the gain?

Public Return

What does the public receive in exchange?

How many permanent local jobs are guaranteed?

What wages are guaranteed?

What local hiring is guaranteed?

What tax revenue is guaranteed?

What local procurement is guaranteed?

What environmental protections are guaranteed?

What community benefits are guaranteed?

Will waste heat, public broadband, workforce training, emergency service funding, or infrastructure benefits be provided?

Are these benefits enforceable?

Clawbacks and Enforcement

What happens if job promises are not met?

What happens if local hiring promises are not met?

What happens if tax revenue is lower than projected?

What happens if environmental limits are exceeded?

What happens if water use exceeds projections?

What happens if power demand increases?

What happens if ownership changes?

What happens if tenants change?
What happens if the project is sold, delayed, cancelled, automated, or abandoned?
Can subsidies be recovered?
Can tax benefits be cancelled?
Can future phases be paused?
Can permits be reviewed?

Time Limits and Review

How long does each subsidy last?
Does it decline over time?
Can it be renewed?
Does renewal require public approval?
Are there scheduled public reviews?
Can the subsidy be ended if public needs change?
Can the subsidy be adjusted if the company becomes more profitable than expected?
Will future councils or governments be locked into the agreement?

Transparency

Will all subsidy agreements be public?
Will annual subsidy values be reported?
Will job and tax performance be reported?
Will public costs be updated over time?
Will utilities disclose ratepayer impacts?
Will governments disclose staff time and administrative costs?
Will independent audits be required?
Will the public be able to compare promised benefits with actual results?

Red Flags

A tax incentive or public subsidy proposal deserves greater scrutiny when the public hears:
"No direct public funding is involved."
"The project will pay for itself through growth."
"Incentives are needed to stay competitive."
"Details are commercially sensitive."
"The project will expand the tax base."
"Utility rates are handled separately."
"Infrastructure upgrades will benefit the broader region."
"Public costs will be offset over time."
"Clawbacks are not necessary because the company is committed."
"The project would not happen without incentives."
"Tax breaks are temporary."
"Economic benefits will outweigh the costs."

A tax break is public money.

A discounted rate is public support.

A road built for one facility is a subsidy.

A utility upgrade paid by ratepayers is not free.

A promise without a clawback is not protection.

What Communities Should Ask For

Before approval, communities should ask for:

A complete public subsidy ledger.

Disclosure of all tax incentives, exemptions, abatements, rebates, freezes, grants, loans, guarantees, land discounts, and utility discounts.

Disclosure of all public infrastructure costs.

Disclosure of all ratepayer impacts.

Identification of every subsidy recipient and ultimate beneficiary.

A full public cost-benefit analysis.

A public cost-per-permanent-job calculation.

A gross and net tax revenue projection.

A public return on investment assessment.

A comparison with alternative public uses of the same money, land, water, electricity, and infrastructure capacity.

Legally binding job, wage, local hiring, procurement, environmental, reporting, and community benefit commitments.

Clawback provisions.

Time limits.

Scheduled public reviews.

Independent audits.

Annual public reporting of subsidies, costs, jobs, taxes, compliance, and public benefits.

Clear penalties and cancellation rights if promises are not met.

The Public Interest Standard

No data center should receive tax incentives, discounted utilities, public infrastructure, grants, loans, or other public subsidies until the full public cost is disclosed, the recipient is identified, the public return is measurable, and clawbacks are legally enforceable.

A community should not be asked to subsidize private digital infrastructure with invisible costs, confidential agreements, or vague promises of future growth.

If the project needs public support, then the public is part of the project.

And if the public is part of the project, the public has the right to see the deal.

19 - Infrastructure Costs and Ratepayer Burden

A data center does not connect itself to the world.

It requires roads, power lines, substations, transformers, water pipes, sewer capacity, stormwater systems, emergency access, fire protection, communications networks, fuel routes, construction staging, maintenance access, and sometimes major regional infrastructure upgrades.

These costs may not appear in the headline investment number.

A company may announce billions of dollars in private spending while the public quietly pays for road widening, water capacity, sewer upgrades, grid reinforcement, emergency services, fire equipment, planning staff, inspections, monitoring, or utility expansion. Some costs may fall on municipal taxpayers. Some may fall on provincial, state, or federal governments. Some may be folded into utility rates. Some may be delayed for years. Some may be hidden in "regional growth" budgets. Some may be justified as general infrastructure even when the immediate trigger is the data center.

The public should not ask only:

What will the company build?

The better question is:

What must the public system build, expand, maintain, or pay for because this project exists?

A data center is not only a development application. It is a demand placed on public and regulated infrastructure.

The Public Bill Is Not Always Obvious

Infrastructure costs can be difficult to see because they are often spread across agencies, departments, utilities, authorities, and levels of government.

A municipality may assess roads and zoning. A utility may assess grid connection. A water authority may assess supply. A sewer department may assess capacity. A fire department may assess response needs. A transportation agency may assess highway access. A province, state, or federal government may fund larger upgrades. Each body may see only part of the cost.

The public experiences the whole bill.

If a data center requires a new substation, that cost may appear in utility planning rather than the development agreement. If transmission upgrades are needed, they may be recovered through electricity rates. If water pipes are upsized, the cost may be assigned to a capital budget. If road improvements are needed, they may be justified as regional growth. If fire services need specialized training or equipment, the cost may appear later in a municipal budget. If emergency planning becomes more complex, staff time may simply be absorbed.

A project should not be allowed to look affordable because the cost is fragmented.

The public should ask for one complete infrastructure cost statement before approval.

Direct Costs and Indirect Costs

Direct costs are the obvious costs required to connect or service the project.

These may include access roads, site entrances, utility connections, water lines, sewer connections, stormwater systems, substations, transformers, distribution lines, transmission connections, and emergency access.

Indirect costs are easier to miss.

These may include upstream grid reinforcement, treatment plant expansion, reservoir capacity, road maintenance, bridge upgrades, traffic control, snow clearing, emergency service expansion, fire equipment, hazardous-material training, public monitoring systems, staff time, legal review, environmental enforcement, utility administration, planning studies, and future replacement costs.

A data center may pay some direct costs while the public absorbs indirect ones.

The public should ask whether both categories have been counted.

Ratepayer Burden

Ratepayer burden occurs when infrastructure costs are recovered through utility bills rather than direct charges to the project.

If a data center requires grid upgrades, water system expansion, sewer capacity, treatment infrastructure, or transmission reinforcement, those costs may be spread across all users. Residents, farms, small businesses, schools, hospitals, municipalities, and future customers may pay more over time, even if they receive little direct benefit.

This can make a private project appear less expensive than it is.

Instead of the company paying the full cost at the time of development, the cost may be socialized through electricity rates, water rates, sewer rates, service charges, connection fees, or future capital plans.

The public should ask whether the data center is paying the full cost of the capacity it requires.

A rate increase is still a public contribution, even when it arrives through a utility bill instead of a tax bill.

Grid Reinforcement and Electrical Infrastructure

Electricity infrastructure is often one of the largest hidden costs.

A data center may require new substations, transformers, switchyards, transmission lines, distribution upgrades, protection systems, control systems, land acquisition, rights-of-way, vegetation clearing, grid studies, reserve capacity, new generation, or backup arrangements.

The public should ask who pays for each part.

Does the developer pay only for the connection from the site to the nearest grid point?

Does the utility pay for upstream upgrades?

Are transmission costs spread across ratepayers?

Are substations sized for the project alone or for future expansion?

Are new lines being justified by the data center but paid for as general grid improvement?

Will local electricity users face higher bills?

Will public agencies pay through their own utility costs?

Grid costs should not be hidden inside technical proceedings that ordinary residents never see.

If the project requires major electrical infrastructure, the public should be told plainly.

Water and Sewer Infrastructure

Water and sewer capacity are also public systems.

A data center may require larger water mains, new pumps, wells, reservoirs, treatment capacity, pressure upgrades, reclaimed water systems, industrial water lines, sewer expansion, wastewater treatment capacity, discharge infrastructure, stormwater systems, monitoring equipment, or drought planning.

Even when a facility claims low water use, the system may still need to be built for peak demand, fire suppression, emergency use, construction needs, future phases, or full buildout.

The public should ask whether existing water and sewer systems can serve the project without harming existing users or delaying future community growth.

Will housing capacity be reduced?

Will farms, local businesses, or public facilities compete for capacity?

Will water or sewer rates rise?

Will the project use infrastructure capacity that was intended for residents?

Will the developer pay for upgrades, or will costs be recovered from all users?

A community should not discover after approval that its next water or sewer rate increase was partly caused by a private industrial load.

Roads, Bridges, and Transportation Infrastructure

Data centers can require major transportation support, especially during construction.

Heavy trucks may carry concrete, steel, generators, transformers, cooling systems, fuel tanks, batteries, electrical equipment, road materials, and construction machinery. Oversized loads may require road widening, turning-radius changes, bridge strengthening, traffic signals, intersection upgrades, shoulder improvements, culvert replacement, rail coordination, escort vehicles, or temporary closures.

Once the facility is operating, transportation impacts may continue through maintenance, security, fuel deliveries, equipment replacement, snow clearing, emergency access, and future expansion.

The public should ask who pays for road and bridge upgrades, and who pays for increased maintenance.

If the project accelerates road wear, the developer should contribute to repair. If rural roads are upgraded primarily for the facility, the public should know whether those roads are being built for the community or for the data center.

Emergency Services and Fire Capacity

A data center may require more from emergency services than an ordinary building.

Fire departments may need training for high-voltage systems, battery fires, fuel storage, diesel generators, gas turbines, chemical suppression systems, cooling systems, electrical rooms, confined spaces, hazardous runoff, security barriers, and large industrial buildings. Emergency medical services may need site access protocols. Police may need security coordination. Emergency managers may need plans for cyber incidents, outages, fires, spills, evacuations, or grid emergencies.

The public should ask whether existing emergency services can support the facility.

Will the fire department need new equipment?

Will additional water supply or fire flow be required?

Will specialized training be needed?

Will response times be affected?

Will mutual aid agreements be required?

Will emergency planning costs increase?

Will the developer pay for these costs?

A facility's private risk should not become an unfunded public safety obligation.

Public Staff Time and Administrative Capacity

Infrastructure burden is not only physical.

Large projects consume public staff time. Planners, engineers, lawyers, utility staff, environmental officers, fire officials, emergency managers, inspectors, communications staff, council members, regulators, and consultants may spend months or years reviewing, negotiating, monitoring, and enforcing a project.

That time has value.

If a municipality or public agency is small, a data center proposal may dominate staff capacity and delay other public work. Housing approvals, local infrastructure planning, environmental enforcement, public engagement, small business support, and ordinary municipal services may be pushed aside.

The public should ask whether the developer is paying the true administrative cost of the project.

Application fees should reflect the complexity of the review. Independent consultants should be paid for by the applicant but chosen by the public authority. Monitoring and enforcement should be funded before the project begins.

Maintenance and Replacement Costs

Infrastructure is not paid for once.

Roads wear out. Pipes age. Pumps need replacement. Substations require maintenance. Transformers fail. Fire equipment must be replaced. Monitoring systems need calibration. Stormwater systems require cleaning. Emergency plans need updates. Staff need training. Utility systems need renewal.

A data center may contribute to initial construction costs while the public inherits long-term maintenance and replacement costs.

The public should ask who pays over the full life of the facility.

If infrastructure is built primarily for the project, long-term maintenance should be included in the development agreement. If a road is widened for heavy construction traffic, repair obligations should be clear. If a water line is oversized for future data center expansion, the carrying cost should not fall silently on residents.

A one-time payment does not settle a decades-long burden.

Existing Infrastructure and Deferred Maintenance

A project should be evaluated against the current condition of local infrastructure.

Many communities already have aging roads, old water mains, limited sewer capacity, strained fire services, grid constraints, bridge repair backlogs, stormwater problems, or underfunded maintenance. A data center may be proposed into a system that is already struggling.

The public should ask whether existing infrastructure is strong enough to support the project without worsening current problems.

Will the project accelerate replacement needs?
Will it compete with overdue repairs?
Will public funds be redirected from existing neighbourhoods?
Will residents be told to wait while infrastructure is upgraded for a new industrial user?
Will the project use capacity that the community needs for housing, schools, hospitals, farms, or climate adaptation?

A data center should not be allowed to leap ahead of existing public needs simply because it arrives with a large investment announcement.

Oversizing and Future Development

Infrastructure built for a data center may be larger than the first project requires.

A road may be widened for future phases. A water line may be sized for a campus. A substation may be built for additional facilities. A transmission corridor may enable a larger industrial zone. Sewer upgrades may support future development. Emergency planning may assume a cluster rather than a single site.

Oversizing is not automatically wrong, but it must be disclosed.

The public should know whether infrastructure is sized for the current project, future expansion, additional data centers, industrial clustering, housing growth, or general community needs.

If the public pays for extra capacity, the public should know who benefits from it and whether that capacity will serve public priorities or private expansion.

Development Charges and Cost Recovery

Many communities use development charges, impact fees, connection fees, off-site levies, utility contributions, or servicing agreements to recover infrastructure costs from new development.

The public should ask whether these tools are strong enough for data centers.

A standard development charge designed for ordinary commercial or industrial users may not reflect the unusual electricity, water, cooling, road, emergency, and monitoring demands of a data center. If fees are too low, the public may subsidize the gap.

Communities should ask whether special cost-recovery rules are needed for large-scale digital infrastructure.

If a project creates extraordinary infrastructure demands, ordinary fees may not be enough.

Core Questions

Full Infrastructure Cost

What infrastructure is required for the project?
What infrastructure is required for the first phase?
What infrastructure is required for full buildout?
What infrastructure is required off site?
What infrastructure is required upstream or downstream from the project?
What direct costs have been identified?
What indirect costs have been identified?
Has a full infrastructure cost statement been published?

Electricity and Grid

Will the project require new substations?
Will it require transmission lines?
Will it require distribution upgrades?
Will it require transformer upgrades?
Will it require grid reinforcement?
Will it require new generation or reserve capacity?
Who pays for each electrical upgrade?
Will costs be recovered through electricity rates?
Will residential, farm, school, hospital, municipal, or small business ratepayers pay more?
Are upgrades sized for the project, future phases, or additional development?

Water and Sewer

Will new water pipes be required?
Will new wells, pumps, reservoirs, treatment capacity, or pressure systems be required?
Will sewer upgrades be required?
Will wastewater treatment capacity be required?
Will stormwater upgrades be required?
Will reclaimed water or industrial water systems be required?
Who pays for each upgrade?
Will water or sewer rates increase?
Will the project use capacity needed for housing, agriculture, public services, or future growth?

Roads and Transportation

Will roads need to be widened?
Will intersections need upgrades?
Will bridges need strengthening?
Will culverts, shoulders, access roads, traffic signals, or turning lanes be required?
Will construction traffic damage local roads?
Who pays for construction-related road wear?
Who pays for long-term road maintenance?

Will transportation upgrades primarily serve the project or the public?

Emergency Services

Can existing fire services support the facility?

Can existing emergency medical services support it?

Can existing police and emergency management capacity support it?

Will specialized fire equipment be required?

Will battery, fuel, chemical, high-voltage, or data center-specific training be required?

Will additional water supply or fire flow be required?

Will mutual aid agreements be needed?

Who pays for new emergency capacity?

Public Administration

How much municipal, utility, regulatory, legal, engineering, fire, environmental, and emergency planning staff time will the project require?

Will the developer pay for independent public review?

Will application fees cover the true cost of review?

Will monitoring and enforcement be funded?

Will the project delay other public work?

Will public agencies need additional staff?

Who pays for that capacity?

Maintenance and Replacement

Who maintains new roads, pipes, substations, stormwater systems, emergency equipment, monitoring systems, and other infrastructure?

Who pays for replacement when infrastructure ages?

Are long-term maintenance costs included in the agreement?

Are lifecycle costs publicly disclosed?

Will residents inherit maintenance obligations after the developer pays initial connection costs?

Existing Infrastructure Condition

What is the current condition of local roads, bridges, water systems, sewer systems, stormwater systems, emergency services, and grid infrastructure?

Are any systems aging, over capacity, underfunded, or scheduled for replacement?

Will the project accelerate repair or replacement needs?

Will the project redirect funds from existing infrastructure priorities?

Will the project delay needed upgrades for residents?

Oversizing and Future Growth

Is infrastructure being oversized?

If so, why?

Who requested the extra capacity?

Who pays for the extra capacity?

Will it serve future phases?
Will it serve additional data centers?
Will it serve general community growth?
Will the public have control over how extra capacity is used?
Could oversized infrastructure create pressure for further industrial development?

Ratepayer and Taxpayer Impact

Will electricity rates increase?
Will water rates increase?
Will sewer rates increase?
Will transmission charges increase?
Will distribution charges increase?
Will infrastructure fees increase?
Will property taxes increase?
Will development charges increase?
Will utility debt increase?
Will municipal borrowing increase?
Will public grants be used?
Will future residents pay for today's infrastructure decisions?
Has a ratepayer and taxpayer impact assessment been completed?

Cost Recovery

Will the developer pay the full cost of infrastructure required by the project?
Are development charges, impact fees, connection fees, off-site levies, or servicing agreements sufficient?
Are special cost-recovery rules needed?
Are cost overruns covered by the developer or the public?
Are bonds, guarantees, deposits, or letters of credit required?
Can costs be recovered if the project is delayed, cancelled, sold, or abandoned?

Red Flags

An infrastructure cost or ratepayer burden proposal deserves greater scrutiny when the public hears:

"Existing infrastructure can accommodate the project."
"Upgrades will benefit the broader community."
"Costs will be handled through normal utility processes."
"The developer will pay its fair share."
"Rate impacts are expected to be minimal."
"Infrastructure will support future growth."
"Grid upgrades are outside the scope of this approval."
"Water and sewer capacity will be addressed later."
"Emergency services can use existing resources."
"Road impacts are temporary."

"Maintenance costs will be managed through ordinary budgets."

Fair share is not a number.
Normal utility process is not public disclosure.
Future growth is not a benefit unless the public chooses it.
A ratepayer charge is still a public cost.
An infrastructure upgrade is not free because it appears in someone else's budget.

What Communities Should Ask For

Before approval, communities should ask for:
A complete infrastructure cost assessment.
A direct and indirect cost statement.
A full-buildout infrastructure assessment.
A grid reinforcement and ratepayer impact assessment.
A water and sewer capacity and ratepayer impact assessment.
A road, bridge, and transportation cost assessment.
An emergency services capacity and funding assessment.
A public administration and enforcement cost assessment.
A lifecycle maintenance and replacement cost assessment.
An existing infrastructure condition report.
An oversizing and future-capacity disclosure.
A taxpayer and ratepayer impact report.
A cost-recovery agreement.

Development charges, impact fees, connection fees, off-site levies, or special infrastructure charges that reflect the true burden of the project.

Bonds, guarantees, deposits, or letters of credit to protect the public from cost overruns, cancellation, sale, abandonment, or underperformance.

Annual public reporting of infrastructure costs, rate impacts, maintenance obligations, and cost recovery.

Clear legal conditions ensuring the public does not inherit private infrastructure costs.

The Public Interest Standard

No data center should be approved until the public knows what infrastructure it requires, what that infrastructure will cost, who will pay for it, who will maintain it, and whether taxpayers or ratepayers will carry any part of the burden.

A community should not be asked to approve a private development while the public bill is scattered across utility rates, road budgets, water plans, emergency services, staff time, and future maintenance.

The question is not whether the project can be connected.
The question is whether the connection is fair.

If a data center requires substations, transmission lines, water pipes, road widening, sewer upgrades, fire capacity, emergency planning, and grid reinforcement, then the public has the right to ask whether those costs are being paid by the project — or quietly passed to everyone else.

20 - Decommissioning and Exit Plans

Every data center proposal should answer a question that is too often left until the end:

What happens when the data center is no longer useful?

A facility may be promoted as permanent infrastructure, but technology changes. Equipment ages. Tenants leave. Workloads move. Companies merge. Owners sell. Parent companies restructure. Subsidies expire. Cooling systems become obsolete. Power demands shift. Artificial intelligence hardware changes. Cloud architecture changes. Land values change. A facility that looks essential today may become outdated, unprofitable, abandoned, or repurposed tomorrow.

The public should not ask only:

What will this project bring?

The better question is:

What will this project leave behind?

A data center can leave behind buildings, concrete pads, buried pipes, transmission connections, substations, fuel tanks, generators, batteries, cooling systems, refrigerants, chemicals, fire suppression systems, stormwater infrastructure, fencing, security equipment, contaminated soil, obsolete servers, electronic waste, stranded public infrastructure, unpaid taxes, broken job promises, and unresolved liability.

A community should not be expected to clean up a private project after the private value has been extracted.

Decommissioning Should Be Planned Before Approval

Decommissioning is not a problem for later.

It is part of the project from the beginning.

If a facility has a construction plan, it should have an exit plan. If it has a servicing plan, it should have a cleanup plan. If it has a tax incentive agreement, it should have clawbacks. If it has public infrastructure, it should have cost-recovery protections. If it has hazardous materials, it should have removal and disposal requirements. If it has major electrical, cooling, water, or backup systems, it should have a legally enforceable plan for what happens when those systems are retired.

A government should not approve a data center on the assumption that it will operate forever.

Nothing industrial operates forever.

Equipment Ages

Data center equipment has a lifecycle.

Servers are replaced. Cooling systems wear out. Batteries degrade. Diesel generators age. Transformers require maintenance or replacement. Refrigerants may become outdated or restricted. Fire suppression systems may need replacement. Electrical systems may no longer meet standards. Security systems may become obsolete. Hardware may be removed, resold, recycled, scrapped, exported, or abandoned.

The public should ask how equipment retirement will be handled.

Where will obsolete servers go?

How will electronic waste be managed?

How will batteries be recycled or disposed of?

How will refrigerants, coolants, oils, fuels, and chemicals be removed?

How will generator systems be decommissioned?

How will fuel tanks be cleaned or removed?

How will fire suppression systems be safely retired?

A data center should not become a warehouse for obsolete technology because cleanup costs were never secured.

Electronic Waste and Hardware Turnover

Data centers are not static buildings filled with permanent equipment.

Servers, GPUs, networking hardware, storage devices, batteries, cooling equipment, cables, racks, power systems, and control systems may be replaced many times over the life of a facility. In AI-focused facilities, hardware turnover may be especially rapid as newer chips, denser racks, and more specialized systems are introduced.

The public should ask how much electronic waste the facility is expected to generate during normal operations, not only at closure.

Where will retired equipment go?

Will it be reused, resold, recycled, exported, stored, destroyed, or landfilled?

Will storage devices be securely wiped or physically destroyed?

Will batteries be recycled safely?

Will rare earths, metals, plastics, circuit boards, cables, cooling components, and hazardous materials be recovered?

Will any e-waste be shipped to jurisdictions with weaker labour, health, or environmental protections?

Will the company publicly report annual equipment turnover and e-waste volumes?

A data center should not be allowed to present itself as clean digital infrastructure while exporting its waste burden somewhere else.

Electronic waste should be counted as part of the facility's environmental footprint.

Tenants May Leave

A facility may be built for one tenant or a group of tenants.

Those tenants may leave.

Cloud providers may relocate workloads. AI companies may move to newer facilities. Government contracts may expire. Crypto operations may shut down. Corporate clients may consolidate elsewhere. Tenants may be acquired, bankrupt, sanctioned, or restructured. The facility may be left partially occupied, underused, or dependent on different tenants with different impacts.

The public should ask what happens if the original tenant mix changes.

Can the facility shift to more energy-intensive uses?

Can it shift to crypto mining?

Can it shift to AI training?

Can it shift to surveillance, policing, military, or foreign-controlled uses?

Can it shift to tenants with higher water, power, heat, or backup demands?

Can it sit mostly empty while still receiving tax benefits?

Can the owner keep public subsidies if promised tenants never arrive?

An approval should not allow one public-interest case to be made for the original proposal and a very different use to operate later without review.

Companies Sell and Restructure

A data center may change hands.

The applicant may sell the land. The developer may sell the building. The operator may be replaced. The parent company may merge. A private equity firm may acquire the asset. A real estate investment trust may take ownership. A foreign company may buy the facility. Lenders may take control after default. A local subsidiary may be dissolved.

If public obligations are attached only to the original applicant, they may become difficult to enforce after ownership changes.

The public should ask whether all decommissioning, cleanup, subsidy, reporting, environmental, and community obligations survive sale, merger, transfer, foreclosure, bankruptcy, restructuring, or tenant change.

No company should be able to escape public obligations by changing the name on the paperwork.

Obsolescence and Repurposing

Technology changes quickly.

A facility designed for one generation of servers may not suit the next. AI hardware may require different cooling. Energy density may increase. Tenants may demand new electrical systems. A facility may become less competitive if newer data centers are built elsewhere. A site may be repurposed for different industrial uses.

The public should ask what uses are allowed if the data center becomes obsolete.

Can the building become a warehouse?

Can it become a crypto-mining operation?

Can it become a high-density AI training facility?

Can it become a battery storage site?

Can it become a private power facility?

Can it become a surveillance or defence contractor site?

Can it become a general industrial site without new review?

Repurposing may be beneficial in some cases. Reusing buildings can avoid demolition and waste. But repurposing should not become a back door for uses the public never approved.

The exit plan should define which future uses require new public review.

Stranded Infrastructure

A data center may require expensive infrastructure that remains even if the facility fails.

Roads may be widened. Water pipes may be upsized. Sewer systems may be expanded. Substations may be built. Transmission lines may be constructed. Emergency services may be

expanded. Public debt may be taken on. Utilities may invest in capacity. Land may be rezoned. A region may reorganize itself around the project.

If the facility closes, the public may be left with stranded infrastructure.

That infrastructure may be underused, costly to maintain, or designed for industrial expansion the community no longer wants. Ratepayers may still pay for grid upgrades. Taxpayers may still pay for roads. Municipalities may still maintain water and sewer systems. Emergency services may still carry equipment costs. Public agencies may still service debt.

The public should ask what happens if the project is delayed, cancelled, downsized, underused, sold, or closed.

Who pays for infrastructure that was built for a project that no longer delivers the promised benefits?

Environmental Cleanup

A data center may not look like a heavy industrial site, but it can still create environmental cleanup issues.

Fuel storage, diesel generators, gas turbines, batteries, transformers, coolants, refrigerants, fire suppression systems, water-treatment chemicals, cleaning agents, stormwater systems, and construction materials can all create contamination risks if improperly managed, leaked, spilled, burned, abandoned, or demolished.

The public should ask for a decommissioning environmental assessment.

What substances will need to be removed?

What soil testing will be required?

What groundwater testing will be required?

What stormwater systems will need to be cleaned?

What fuel tanks will be removed?

What batteries will be recycled?

What refrigerants will be captured?

What electronic waste will be handled?

What buildings, slabs, pipes, cables, foundations, fences, and utility systems will remain?

Cleanup obligations should be specific, funded, and enforceable.

Data Disposal and Digital Exit

Decommissioning is not only physical.

If a data center closes, changes tenants, sells, or repurposes, there must be a plan for data transfer, data deletion, encryption key control, backup destruction, public-sector continuity, privacy protection, and records accountability.

The public should ask what happens to public data, health data, school data, court data, policing data, Indigenous data, personal data, and sensitive commercial data if the facility changes hands or shuts down.

Can data be moved safely?

Can public services continue?

Are backups deleted?

Are storage devices wiped or destroyed?

Are logs and metadata handled properly?

Can tenants leave without data loss?

Can governments retrieve their records?

Can data be trapped by vendor lock-in, bankruptcy, litigation, foreign legal orders, or unpaid bills?

A shutdown plan that deals only with buildings and equipment is incomplete.

The data must have an exit plan too.

Bonds, Reserve Funds, and Financial Security

A promise to clean up later is not enough.

The public should require financial security before approval.

That may include decommissioning bonds, environmental bonds, reclamation funds, letters of credit, parent-company guarantees, insurance, escrow accounts, reserve funds, or other legally enforceable financial instruments.

The amount should be based on independent estimates of full cleanup, equipment removal, hazardous material handling, site restoration, infrastructure removal, data disposal, and long-term monitoring where needed.

The financial security should be updated regularly. Cleanup costs can rise. Facilities can expand. Equipment can change. Inflation can increase costs. New hazards can emerge.

A bond that is adequate on opening day may be inadequate twenty years later.

The public should not rely on the future goodwill or solvency of the company.

Decommissioning Triggers

An exit plan should define when decommissioning obligations begin.

Triggers may include closure, prolonged inactivity, reduced occupancy, bankruptcy, abandonment, failure to maintain permits, major tenant loss, unpaid taxes, environmental violations, change of use, sale, removal of equipment, failure to meet job commitments, failure to maintain financial security, or expiration of public agreements.

Without clear triggers, a facility may sit in limbo.

A partially empty facility may remain fenced, lit, underused, deteriorating, and exempt from full cleanup because the owner claims future use is possible.

The public should ask how long a facility can remain idle before cleanup, repurposing, or review is required.

Site Restoration

The public should know what condition the site must be returned to.

Will buildings be removed?

Will foundations be removed?

Will roads be removed?

Will fencing be removed?

Will underground pipes and cables be removed?

Will soil be restored?

Will farmland be reclaimed?

Will wetlands be restored?

Will vegetation be replanted?

Will stormwater systems remain?

Will substations or transmission connections stay in place?

Will the site be prepared for future industrial use, community use, agriculture, conservation, or redevelopment?

Restoration should match the community's long-term land-use goals, not only the cheapest exit for the company.

Public Reporting and Oversight

Decommissioning should not occur behind closed gates.

The public should receive notice when equipment is removed, major tenants leave, operations are reduced, ownership changes, public data is migrated, hazardous materials are removed, or cleanup begins.

Regulators should inspect the site. Independent experts should verify cleanup. Communities should be able to review reports. Indigenous governments should be involved where rights, land, water, or data are affected. Farmers, neighbours, utilities, and emergency services should be notified where they may be affected.

The public should not have to discover abandonment after the jobs disappear and the lights stay on behind the fence.

Core Questions

Lifespan and Obsolescence

What is the expected lifespan of the facility?

What is the expected lifespan of the servers?

What is the expected lifespan of cooling systems?

What is the expected lifespan of batteries, generators, transformers, fire suppression systems, and other major equipment?

What technology changes could make the facility obsolete?

Can the facility be economically or technically upgraded?

What happens if it cannot be upgraded?

Has an obsolescence risk assessment been completed?

Tenants and Use Changes

What happens if major tenants leave?

What happens if promised tenants never arrive?

Can the facility change tenants without public notice?

Can the facility shift to AI training, crypto mining, surveillance, defence, policing, or other high-impact uses?

Can the facility increase energy, water, cooling, heat, emissions, or backup demands through a tenant change?

What changes require public review?

What changes trigger new environmental, data, grid, water, or land-use assessment?

Ownership Changes

What happens if the project is sold?

What happens if the operator changes?

What happens if the parent company changes?

What happens if the company merges, restructures, defaults, or enters bankruptcy?

Do all obligations survive sale or transfer?

Can public subsidies transfer?

Can water rights, grid agreements, and tax incentives transfer?

Can a foreign owner acquire the facility without public review?

Who remains liable after ownership changes?

Physical Decommissioning

What equipment must be removed at closure?

Who removes servers, batteries, generators, fuel tanks, transformers, cooling systems, fire suppression systems, cables, pipes, and security systems?

Will buildings be demolished or reused?

Will foundations be removed?

Will underground infrastructure be removed?

Will roads, fencing, lighting, and stormwater systems be removed?

Who verifies removal?

Where will removed materials go?

Environmental Cleanup

What hazardous or regulated materials may remain on site?

Will fuel tanks be removed and tested?

Will soil be tested?

Will groundwater be tested?

Will stormwater systems be tested?

Will batteries be recycled?

Will refrigerants and coolants be captured and properly disposed of?

Will fire suppression chemicals be removed?

Will electronic waste be recycled or disposed of safely?

Who pays for cleanup?

What standards apply?

Data Exit

What happens to data when the facility closes, sells, changes tenants, or changes use?
Can public agencies retrieve their data?
Can tenants retrieve their data?
How will storage devices be wiped, destroyed, or certified?
How will backups be deleted?
How will logs and metadata be handled?
Who controls encryption keys during exit?
How will public-sector data continuity be protected?
Can data be trapped by vendor lock-in, bankruptcy, litigation, or foreign legal process?

Stranded Infrastructure

What public infrastructure was built for the project?
What happens to roads, pipes, substations, transmission lines, water systems, sewer systems, stormwater systems, and emergency capacity if the facility closes?
Who pays remaining debt?
Who pays maintenance?
Can infrastructure be repurposed for public benefit?
Can unused capacity be reassigned to housing, public services, agriculture, or local businesses?
Will ratepayers continue paying for infrastructure built for a closed or underused facility?

Financial Security

Is there a decommissioning bond?
Is there an environmental bond?
Is there a reclamation fund?
Is there a reserve fund?
Is there a letter of credit?
Is there a parent-company guarantee?
Is there insurance for cleanup and abandonment?
Who holds the financial security?
How much is required?
How was the amount calculated?
Is it independently verified?
Is it updated regularly?
Can it be accessed if the company refuses or cannot pay?

Decommissioning Triggers

What events trigger decommissioning obligations?
Closure?
Prolonged inactivity?
Major tenant loss?
Bankruptcy?

Sale?
Abandonment?
Failure to maintain permits?
Failure to maintain financial security?
Environmental violation?
Unpaid taxes?
Change of use?
How long can the facility sit idle before action is required?
Can partial decommissioning be required?
Can the public force review if the site becomes underused or abandoned?

Site Restoration

What condition must the site be returned to?
Will the site be restored to industrial use, agricultural use, ecological use, public use, or another agreed use?
Will farmland be reclaimed?
Will wetlands or habitat be restored?
Will soil health be restored?
Will vegetation be replanted?
Will monitoring continue after restoration?
Who decides whether restoration is complete?
Will the public have access to restoration reports?

Public Oversight

Will decommissioning plans be public?
Will closure or major operational reduction require public notice?
Will ownership changes require public notice?
Will tenant changes require public notice?
Will hazardous material removal be reported?
Will data disposal be certified?
Will cleanup reports be public?
Will independent inspections be required?
Will Indigenous governments, municipalities, utilities, neighbours, farmers, and emergency services be consulted where affected?

Red Flags

A decommissioning or exit proposal deserves greater scrutiny when the public hears:
"Decommissioning will be addressed later."
"The facility is expected to operate indefinitely."
"Equipment will be upgraded as needed."
"Future owners will assume responsibility."
"Closure is unlikely."
"Cleanup will follow applicable laws."

"The site can be repurposed."
"Tenants may change over time."
"Financial security is not necessary."
"Existing corporate resources are sufficient."
"Data deletion is handled by standard procedures."

Indefinite operation is not a plan.
Future owners are not a guarantee.
Applicable law may be weaker than public need.
A repurposed site may create new impacts.
A cleanup promise without secured money is not protection.

What Communities Should Ask For

Before approval, communities should ask for:
A full decommissioning plan.
A physical equipment removal plan.
An environmental cleanup plan.
A hazardous materials and electronic waste management plan.
A battery, generator, fuel tank, refrigerant, coolant, transformer, and fire suppression system retirement plan.
A data exit and certified deletion plan.
A public-sector data continuity plan where public data is involved.
A tenant departure and use-change review process.
An ownership transfer obligation plan.
A stranded infrastructure assessment.
A site restoration plan.
A decommissioning trigger framework.
A financial security requirement, including bonds, reserve funds, letters of credit, insurance, or parent-company guarantees.
Independent cost estimates for cleanup and restoration.
Regular updates to financial security amounts.
Public reporting requirements for closure, equipment removal, data disposal, hazardous material handling, cleanup, and restoration.
Clear legal authority for governments to access financial security and complete cleanup if the owner fails to act.

The Public Interest Standard

No data center should be approved until the public knows what happens when the equipment ages, tenants leave, ownership changes, technology shifts, subsidies expire, or the facility becomes obsolete.

A community should not inherit a stranded building, unpaid infrastructure, obsolete equipment, contaminated land, abandoned batteries, empty promises, or public debt after private value has moved on.

The end of the project is part of the project.

If a company wants permission to build, connect, consume, operate, and profit, it should also prove that it can leave responsibly.

No exit plan, no approval.

Part Five: Accountability After Approval

21 - Monitoring, Reporting, and Enforcement

A data center proposal is built on predictions.

Predicted water use.

Predicted power demand.

Predicted noise.

Predicted emissions.

Predicted traffic.

Predicted heat.

Predicted jobs.

Predicted tax revenue.

Predicted ecological impacts.

Predicted public benefits.

But predictions are not proof.

Once a data center is approved, constructed, connected, and operating, the public should not be expected to rely on promises, averages, annual summaries, company press releases, or complaint forms that disappear into private systems.

The public should be able to verify what is actually happening.

The question is not only:

What did the company promise before approval?

The better question is:

Who measures actual performance, how often is it measured, who sees the data, what happens when limits are exceeded, and can the public confirm that enforcement occurred?

Monitoring, reporting, and enforcement are the difference between a condition written on paper and a condition that actually protects the community.

Approval Is Not Accountability

A permit condition is only as strong as the system built to enforce it.

If a data center is allowed to use a certain amount of water, someone must measure actual water use. If it has a power demand limit, someone must track actual load. If it has noise limits, someone must monitor real sound levels at meaningful locations. If generator testing is restricted, someone must verify when generators run. If emissions are capped, someone must measure or audit emissions. If ecological impacts are predicted to be minimal, someone must monitor plants, animals, water, soil, and habitat after construction.

A public authority should not grant approval and then assume compliance.

Compliance must be demonstrated.

Monitoring should begin before construction, continue during construction, and remain in place during operation, expansion, emergency events, and decommissioning.

A community should not have to prove harm after the fact with screenshots, cellphone videos, sleepless nights, dead vegetation, stressed livestock, or public records requests.

Real-Time Data Versus Company Summaries

Reporting can be designed to inform the public, or it can be designed to manage the public.

A company summary may say that water use remained within approved limits, sound levels were compliant, emissions were acceptable, and complaints were resolved. But summaries may hide timing, peaks, frequency, location, severity, duration, and repeated patterns.

The public should ask whether data will be reported in real time, near real time, monthly, quarterly, annually, or only when the company chooses to summarize it.

Some information may legitimately require protection for security or privacy reasons. But basic public-interest data should be available in a form the public can understand and verify.

Water use, electricity demand, generator runtime, emissions events, sound levels, heat discharge, thermal discharge, complaint totals, exceedances, enforcement actions, and monitoring results should not disappear into confidential reports.

If the public bears the impacts, the public should see the data.

Monitoring Must Measure the Right Things

Monitoring should match the risks.

A data center that uses water should monitor withdrawal, consumption, discharge, temperature, water quality, seasonal use, drought use, and full-buildout demand.

A data center that uses large amounts of electricity should monitor power demand, peak load, generator runtime, curtailment events, battery operation, backup systems, and grid impacts.

A data center that produces sound should monitor all relevant frequencies, including low-frequency sound, tonal sound, nighttime sound, generator testing, construction noise, vibration, and cumulative sound.

A data center that creates emissions should monitor generator operation, fuel use, particulate matter, nitrogen oxides, greenhouse gases, air quality, testing events, emergency operation, and incidents.

A data center that affects land, wildlife, farms, water, or ecosystems should monitor habitat, livestock, crops, pollinators, birds, bats, amphibians, aquatic life, soil, wetlands, runoff, vegetation, and cumulative ecological change where relevant.

Monitoring should not be limited to the easiest measurements.

It should measure the impacts that matter.

Monitoring Locations Matter

A monitor in the wrong place can make a real problem disappear.

Sound measured only at the property line may not show what residents experience inside homes. Air monitoring located away from prevailing winds may miss exposure. Water monitoring at one discharge point may miss downstream effects. Ecological monitoring inside a narrow project boundary may miss impacts on wildlife corridors, farms, wetlands, or waterways. Heat monitoring at the facility wall may miss the surrounding heat island.

The public should ask who selects monitoring locations.

Monitoring locations should include the places where impacts are likely to be experienced: homes, farms, schools, hospitals, care facilities, barns, livestock areas, wetlands, streams, wildlife corridors, public roads, trails, parks, downstream points, and future development areas.

The company should not be the only party deciding where public-interest impacts are measured.

Baseline Data

Communities need baseline data before construction begins.

Without baseline data, it becomes easier for companies or regulators to claim that later problems were pre-existing, unrelated, unproven, or impossible to attribute.

Baseline monitoring should document existing water levels, water quality, air quality, sound levels, nighttime conditions, traffic, wildlife activity, livestock conditions where relevant, vegetation, soil health, wetlands, drainage, temperature, and community conditions before construction.

Baseline data should be public.

A community cannot measure change if it does not know where it started.

Independent Monitoring

Monitoring should not rely entirely on the company being monitored.

Company data may be useful, but public accountability requires independence. Monitoring systems should be installed, audited, or verified by independent experts selected or approved by public authorities, not solely by the developer.

The public should ask:

Who owns the monitors?

Who maintains them?

Who calibrates them?

Who has access to raw data?

Who audits the data?

Who verifies exceedances?

Who investigates complaints?

Who pays for independent review?

Who has authority to require corrective action?

The developer can pay for monitoring, but the public should control the accountability structure.

Public Dashboards and Open Data

Where feasible, data should be published through a public dashboard.

A public dashboard could show water use, power demand, generator testing, emissions events, sound levels, discharge temperature, complaints, exceedances, enforcement actions, and other project-specific indicators. It should use plain language, downloadable data, archives, time stamps, maps, and clear comparison against approved limits.

The dashboard should not be a marketing page.

It should be an accountability tool.

The public should be able to see not only whether the facility is operating within limits, but whether problems are recurring, whether complaints correspond to spikes, whether generator tests occurred as scheduled, whether water use rises during heat waves, whether noise increases at night, whether discharge temperature changes during drought, and whether enforcement follows violations.

If data is delayed, summarized, filtered, or withheld, the public should be told why.

Complaints Are Data

Public complaints should not be treated as nuisances.

Complaints are part of the monitoring system. Residents, farmers, workers, Indigenous communities, nearby businesses, school officials, health-care providers, and local observers may notice problems that formal monitoring misses.

A complaint system should be accessible, public, timely, and enforceable.

People should be able to report noise, vibration, light trespass, odour, air quality, generator operation, water concerns, runoff, traffic, wildlife impacts, livestock stress, heat, dust, safety issues, outages, or other concerns without being dismissed.

Complaints should be logged, categorized, investigated, time-stamped, mapped where appropriate, and compared against monitoring data.

The public should know how many complaints were received, what they concerned, how quickly they were investigated, what was found, and what corrective action was taken.

A complaint process that leads nowhere is not accountability.

Enforcement Must Have Consequences

Monitoring without enforcement is observation.

If a facility exceeds limits, violates conditions, fails to report, underreports, changes operations without notice, ignores complaints, or fails to maintain monitoring systems, there must be consequences.

Those consequences may include warnings, public notices, fines, mandatory mitigation, operating restrictions, generator testing limits, water reductions, lighting changes, noise controls,

additional monitoring, independent audits, suspension of incentives, clawbacks, permit review, denial of future phases, or suspension of operations.

Penalties should be large enough to matter.

A fine that is cheaper than compliance is not enforcement. It is a fee for violation.

Enforcement should be automatic where possible, escalating for repeated or serious violations. The public should be able to see not only that a violation occurred, but what action was taken.

Reporting During Emergencies

Emergency events require special reporting.

During outages, generator operation, battery incidents, fires, chemical releases, spills, cooling failures, water restrictions, heat waves, wildfire smoke, floods, cyber incidents, or emergency curtailment, the public should receive timely notice.

Emergency reporting should identify what happened, when it happened, what systems were involved, what emissions or risks occurred, whether public services were affected, whether residents should take action, what agencies responded, and what follow-up will occur.

Security concerns may limit some details. But security should not be used to hide public health, environmental, or safety information.

If a data center creates an emergency risk, it also creates an emergency communication duty.

Monitoring Future Phases and Expansion

Monitoring should not be frozen at the first phase.

If the facility expands, adds tenants, increases power demand, changes cooling systems, installs more generators, adds batteries, changes water use, alters lighting, changes backup systems, or increases building area, monitoring requirements should expand too.

Future phases should not rely on old data.

Approval conditions should require updated baseline comparisons, updated modelling, new monitoring points, public review, and revised enforcement thresholds before expansion.

A project should not be allowed to grow beyond the monitoring system designed for its first version.

Long-Term Accountability

Data centers may operate for decades.

Monitoring should not end after one year of operation. Some impacts appear slowly. Groundwater changes may take time. Habitat disruption may become visible over seasons. Noise complaints may increase after expansion. Heat island effects may worsen as surrounding land develops. Equipment may get louder as it ages. Backup systems may be tested more often. Tenants may change. Water demand may increase. Public trust may decline if data disappears.

The public should ask how long monitoring continues.

For major facilities, monitoring should continue for the life of the project, with public review points built into the approval.

A data center that operates continuously should be accountable continuously.

Core Questions

Water Monitoring

Will water withdrawal be monitored?

Will water consumption be monitored separately from withdrawal?

Will discharge be monitored?

Will discharge temperature be monitored?

Will discharge quality be monitored?

Will water use be reported daily, monthly, seasonally, and annually?

Will peak use be reported?

Will drought-period use be reported?

Will construction water use be reported separately?

Will water data be publicly available in real time or near real time?

Will data be independently audited?

Power Monitoring

Will electricity demand be monitored?

Will peak demand be reported?

Will average demand be reported?

Will full-buildout demand be tracked?

Will cooling-related power demand be reported separately where possible?

Will generator runtime be reported?

Will battery operation be reported?

Will grid curtailment events be reported?

Will outages be reported?

Will public agencies and ratepayers be able to see whether demand matches the approved projections?

Emissions Monitoring

Will generator emissions be monitored?

Will generator testing emissions be reported?

Will emergency operation emissions be reported?

Will fuel use be reported?

Will particulate matter, nitrogen oxides, sulfur dioxide, carbon monoxide, volatile organic compounds, greenhouse gases, or other relevant pollutants be monitored?

Will air quality be monitored near homes, schools, farms, care facilities, and other sensitive locations where relevant?

Will emissions data be independently verified?

Will exceedances trigger public notice?

Noise, Vibration, and Light Monitoring

Will sound be monitored continuously?

Will all relevant frequencies be monitored?

Will low-frequency sound be reported separately?

Will nighttime sound be reported separately?

Will tonal sound and vibration be assessed?

Will generator testing noise be reported separately?

Will construction noise be monitored?

Will monitoring occur at homes, farms, sensitive sites, wildlife areas, and future residential areas where relevant?

Will monitoring be set up at standardized distances?

Will lighting levels and light trespass be monitored?

Will residents be able to compare complaints against actual sound and light data?

Heat and Cooling Monitoring

Will heat rejection be monitored?

Will discharge temperature be monitored?

Will local temperature or heat island effects be monitored?

Will cooling system performance be reported?

Will cooling failures be reported?

Will emergency cooling events be reported?

Will waste heat recovery be monitored if implemented?

Will heat impacts be assessed during heat waves and full-load operation?

Ecological Monitoring

Will wildlife impacts be monitored?

Will livestock impacts be monitored where farms are nearby?

Will crop and soil impacts be monitored where agricultural land may be affected?

Will pollinators, birds, bats, amphibians, aquatic life, wetlands, vegetation, and habitat corridors be monitored where relevant?

Will monitoring continue across seasons?

Will construction impacts and operational impacts be monitored separately?

Will Indigenous ecological knowledge, farmer observations, and community reports be included where appropriate?

Will ecological monitoring results be public?

Public Complaints

How can complaints be submitted?

Can complaints be submitted online, by phone, in writing, and through local offices?

Will complaints be accepted from residents, farmers, Indigenous communities, workers, businesses, schools, health providers, and visitors?

Will complaints be time-stamped?

Will complaints be mapped?

Will complainants receive follow-up?

Will complaints be compared with monitoring data?

How quickly must complaints be investigated?
Will complaint totals and outcomes be public?
What happens if repeated complaints occur despite claimed compliance?

Public Reporting

What data will be public?
Will data be real time, near real time, monthly, quarterly, annual, or summary only?
Will raw data be available?
Will data be downloadable?
Will data be archived?
Will data be presented in plain language?
Will approved limits be shown beside actual measurements?
Will exceedances be clearly marked?
Will enforcement actions be listed?
Will public dashboards be maintained for the life of the project?

Independence and Auditing

Who collects monitoring data?
Who owns the monitoring equipment?
Who maintains and calibrates the equipment?
Who has access to raw data?
Who verifies the data?
Who pays for independent audits?
Who selects the auditors?
How often are audits required?
Are audit reports public?
Can the public authority require additional monitoring?
Can affected communities request additional monitoring points?

Enforcement

What happens if limits are exceeded?
What happens if monitoring equipment fails?
What happens if data is not reported?
What happens if reporting is late?
What happens if the company underreports?
What happens if complaints are not investigated?
What happens if violations repeat?
Are penalties automatic?
Are penalties large enough to matter?
Can operations be restricted?
Can generators be limited?
Can water use be reduced?

Can lighting be changed?
Can noise mitigation be required?
Can tax incentives be suspended?
Can future phases be denied?
Can permits be reopened, suspended, or revoked?

Expansion and Change

Will monitoring requirements increase with future phases?
Will new tenants trigger updated monitoring?
Will increased power demand trigger updated monitoring?
Will changes in cooling systems, generators, batteries, water use, lighting, or emissions trigger public review?
Will monitoring locations be updated as surrounding land develops?
Will future residential, agricultural, or ecological changes be considered?

Red Flags

A monitoring, reporting, or enforcement proposal deserves greater scrutiny when the public hears:
"Compliance will be reported annually."
"The company will monitor its own operations."
"Data will be summarized for the public."
"Real-time reporting is not necessary."
"Monitoring will occur if complaints are received."
"Complaints will be handled through normal channels."
"Enforcement will follow existing processes."
"Details are commercially sensitive."
"Monitoring requirements can be finalized after approval."
"Impacts are expected to remain within permitted limits."
"Future phases will be monitored later."

Annual summaries are not real-time accountability.
Company monitoring is not independent verification.
A complaint system is not enforcement.
A model is not a measurement.
A permit condition is not protection unless violation has consequences.

What Communities Should Ask For

Before approval, communities should ask for:
A full monitoring, reporting, and enforcement plan.
Baseline data collected before construction.
Continuous monitoring of key impacts where appropriate.
Real-time or near real-time public reporting where feasible.

Separate monitoring of water withdrawal, consumption, and discharge.

Separate monitoring of power demand, peak load, generator runtime, and outages.

Separate monitoring of emissions, fuel use, generator testing, and emergency operation.

Full-spectrum sound, vibration, and nighttime monitoring.

Light trespass and dark-sky monitoring.

Heat rejection, cooling performance, and thermal discharge monitoring.

Ecological monitoring where farms, wildlife, wetlands, waterways, crops, soil, or habitat may be affected.

A public complaint system with timelines and reporting.

Public dashboards with plain-language data, downloadable records, archives, and approved limits shown beside actual measurements.

Independent audits.

Public access to raw data where appropriate.

Clear enforcement thresholds.

Automatic penalties for violations.

Escalating consequences for repeated violations.

Permit-review triggers if impacts exceed predictions.

Funding from the developer for public monitoring, auditing, enforcement, and complaint investigation.

Legal authority for regulators to require corrective action, restrict operations, suspend incentives, deny future phases, or reopen approvals.

The Public Interest Standard

No data center should be approved until monitoring, reporting, and enforcement are defined, funded, independent, public, and legally enforceable.

The public should not be asked to accept company summaries in place of real data.

It should not be asked to trust models when actual measurements are possible.

It should not be asked to file complaints into systems that have no deadlines, no transparency, and no consequences.

If a data center uses public water, draws from the public grid, affects public air, creates public noise, alters public landscapes, receives public subsidies, or places burdens on public infrastructure, then the public has the right to see what is happening.

Not once a year.

Not after harm is denied.

Not after expansion is already approved.

But continuously, clearly, and in a form that allows communities to know whether promises are being kept.

Accountability begins where prediction ends.

22 - Emergency Planning

A data center is designed to avoid interruption.

That does not mean it is immune to failure.

A data center can experience fire, explosion, battery failure, diesel spill, chemical release, water contamination, cooling failure, generator malfunction, cyberattack, grid failure, flooding, wildfire, extreme heat, extreme cold, storm damage, structural damage, equipment failure, evacuation needs, or cascading emergencies that involve more than one system at the same time.

The public should not ask only:

Does the facility have an emergency plan?

The better question is:

What emergencies are possible, who responds, who pays, who is notified, what risks affect the surrounding community, and whether local emergency services have the capacity to handle them?

Emergency planning is not only about protecting the servers.

It is about protecting people, workers, first responders, nearby homes, farms, schools, hospitals, roads, water systems, wildlife, air, land, and public services.

A facility that requires public emergency response creates public emergency obligations.

Emergency Planning Before Approval

Emergency planning should happen before approval, not after construction.

A community should not approve a data center and then discover later that the fire department needs specialized equipment, that local water pressure is inadequate for fire suppression, that roads cannot handle evacuation and emergency access at the same time, that battery systems require special training, that diesel storage creates spill risks, that chemical suppression systems require hazardous-material protocols, or that cyber incidents could disrupt public services.

If a facility creates emergency risks, those risks should be assessed before the project is approved.

The emergency plan should be reviewed by local fire departments, emergency medical services, police, emergency management officials, utilities, water authorities, environmental regulators, public health officials, Indigenous governments where relevant, and neighbouring jurisdictions that may be affected.

Emergency planning should not be left entirely to the company.

Fire and Explosion

Data centers contain electrical systems, high-density equipment, batteries, generators, fuel systems, transformers, cooling systems, fire suppression systems, cabling, server rooms, mechanical rooms, and sometimes hazardous materials.

Fire risks may come from electrical faults, overheating equipment, battery thermal runaway, generator failure, fuel leaks, transformer incidents, construction activity, maintenance errors, cooling failure, lightning, wildfire exposure, or other events.

The public should ask what kind of fires are possible and whether local responders are prepared.

A battery fire is not the same as an office fire.
A transformer fire is not the same as a kitchen fire.
A diesel spill fire is not the same as a grass fire.
A server room fire is not the same as a warehouse fire.
A wildfire approaching a data center is not the same as a wildfire approaching an empty field.

Emergency planning must match the actual systems on site.

Battery Failure and Thermal Runaway

Battery systems may support backup power, grid services, peak management, or uninterruptible power. They may also create specialized emergency risks.

Battery failures can involve fire, heat, smoke, toxic gases, explosion risk, reignition, contaminated runoff, evacuation needs, specialized suppression methods, and long-duration response. Depending on the battery chemistry and system design, ordinary firefighting methods may be insufficient or may create additional hazards.

The public should ask whether battery risks have been assessed in detail.

What type of batteries will be used?

Where will they be located?

How large is the system?

What separation distances apply?

What fire suppression system is used?

What gases or toxins could be released?

What water or chemical runoff could result?

Could fire spread to other systems?

Could a battery incident affect nearby homes, farms, roads, waterways, or emergency responders?

Battery storage should not be treated as automatically safe because it is associated with clean energy.

It is still industrial infrastructure.

Diesel, Fuel, and Generator Emergencies

Backup generators require fuel.

That may mean diesel storage tanks, fuel lines, refuelling stations, deliveries, spill containment, leak detection, fire suppression, ventilation, exhaust systems, and emergency operating procedures. Gas turbines or other systems may require different fuel infrastructure and safety planning.

Fuel systems can fail.

Spills can contaminate soil, stormwater, groundwater, wetlands, rivers, sewer systems, roads, and neighbouring properties. Generator fires can produce smoke, emissions, noise, and evacuation

concerns. Fuel deliveries can create traffic and spill risks. Extended outages can increase fuel demand during periods when roads and emergency services may already be strained.

The public should ask how fuel is stored, transported, monitored, contained, and removed during emergencies.

Backup power is not just a reliability feature.

It is also a fuel and fire risk.

Chemical Releases and Fire Suppression Systems

Data centers may use refrigerants, coolants, water-treatment chemicals, corrosion inhibitors, biocides, cleaning agents, transformer oils, battery materials, fire suppression chemicals, inert gases, clean agents, foams, or other substances.

Some may be low risk under normal conditions. Others may create hazards if released, burned, mixed, discharged, or washed into water systems during firefighting.

The public should ask for a chemical inventory and emergency response plan.

What chemicals are on site?

Where are they stored?

What quantities are present?

What happens if they leak?

What happens if they burn?

What happens if fire suppression systems discharge?

Could chemicals enter stormwater, sewer systems, groundwater, wetlands, rivers, farms, or nearby properties?

Are first responders trained and equipped for these substances?

The phrase "standard fire suppression" is not enough.

The public should know what standard means.

Water Contamination and Runoff

Emergencies often become water emergencies.

A fire can produce contaminated runoff. A diesel spill can enter ditches or storm drains. A chemical release can reach groundwater. A battery incident can produce toxic runoff. Flooding can carry contaminants off site. Fire suppression water can move through stormwater systems. Cooling system failures can release treated water or fluids. Construction emergencies can mobilize sediment, fuels, or chemicals.

The public should ask where emergency runoff would go.

Would it enter a river, lake, wetland, ditch, stormwater pond, sewer system, groundwater recharge area, farm field, or neighbouring property?

Can it be contained on site?

Are shutoff valves installed?

Are containment ponds sized for worst-case events?

Can contaminated water be isolated before it leaves the site?

Who tests it?

Who pays for cleanup?

Who notifies downstream users?

A facility should not be approved unless emergency runoff has a destination other than "away."

Cyberattack and Digital Emergencies

A data center emergency may be digital.

A cyberattack can disrupt public services, compromise data, disable security systems, affect cooling controls, interfere with backup systems, lock operators out, trigger ransomware, expose sensitive information, disrupt utilities, or create cascading failures.

If the facility supports public services, health systems, emergency services, courts, schools, utilities, policing, communications, or government operations, a cyber incident can become a public emergency.

The public should ask whether cyberattack scenarios are included in emergency planning.

What happens if the facility is attacked during a heat wave, wildfire, flood, grid emergency, or physical incident?

What happens if systems are offline?

What happens if emergency responders cannot access digital site information?

What happens if public agencies lose access to records?

What happens if backup systems are compromised?

Emergency planning should assume that digital and physical failures can overlap.

Grid Failure and Power Emergencies

Data centers depend on electricity, but they can also affect the grid.

During grid failures, the facility may switch to backup power. During grid stress, it may be asked to reduce load. During major outages, it may continue operating while nearby residents, farms, hospitals, or businesses face power loss. During extended outages, generators may run for long periods, fuel deliveries may increase, emissions may rise, and noise may become continuous.

The public should ask what happens during a grid emergency.

Will the facility reduce load?

Will it be required to curtail operations?

Will it receive priority power?

Will backup generators run?

How long can they run?

How much fuel is stored?

Will fuel deliveries compete with emergency routes?

Will local air quality be affected?

Will residents be notified?

A data center should not weaken community resilience during the very moments when resilience matters most.

Extreme Heat, Cooling Failure, and Heat Waves

Extreme heat can stress both data centers and communities.

During heat waves, cooling demand may rise. Water demand may rise. Power demand may rise. Generator risk may rise. Equipment may operate harder. Workers may face heat stress. Local heat island effects may worsen. Vulnerable residents may be at greater risk. Livestock, crops, and wildlife may already be under stress.

The public should ask how the facility will operate during extreme heat.

Can it reduce workload?

Can it reduce water use during restrictions?

Can it remain safe during cooling failure?

Will emergency cooling increase emissions, noise, or water use?

Will public water or power priority be affected?

Could heat rejected from the facility worsen local conditions?

The emergency plan should consider community heat risk, not only server temperature.

Flood, Stormwater, and Severe Weather

Data centers are vulnerable to flooding, storms, ice, hail, wind, lightning, and drainage failure.

Flooding can damage electrical systems, fuel tanks, batteries, cooling systems, generators, roads, fiber connections, basements, stormwater systems, and emergency access. Stormwater failures can move pollutants off site. Severe weather can disrupt power, access roads, emergency response, and communication.

The public should ask whether flood and storm risk has been assessed under present and future climate conditions.

Is the site in a floodplain?

Could drainage changes increase flooding nearby?

Can emergency vehicles access the site during floods or storms?

Are fuel tanks protected from floating, rupture, or leakage?

Are batteries and electrical systems elevated or protected?

Can stormwater ponds contain contaminated runoff?

Can the site operate safely during extreme weather?

A facility designed for past weather may not be safe in the future climate.

Wildfire and Smoke

In many regions, wildfire risk is increasing.

A data center may be located near grasslands, forests, rural roads, transmission corridors, substations, fuel storage, batteries, or dry vegetation. Wildfire can threaten the facility, while the facility's electrical infrastructure, generators, vehicles, construction activity, or vegetation management may affect local fire risk.

Wildfire smoke can also affect air intake, cooling systems, workers, nearby residents, livestock, and emergency response.

The public should ask whether wildfire risk has been assessed.

Is the site defensible?

Will vegetation be managed?

Could transmission lines increase fire risk?

Could backup generators operate during smoke events?

Would generator emissions worsen already poor air quality?

Can evacuation routes handle both community evacuation and facility emergency traffic?

Are local fire services equipped for a combined wildfire and industrial incident?

Wildfire planning should not end at the property line.

Evacuation and Shelter-in-Place

Some emergencies may require evacuation. Others may require people to stay indoors.

The public should know which scenarios apply.

If there is a chemical release, battery fire, fuel spill, major smoke event, explosion risk, wildfire, flooding, or security incident, who decides whether nearby residents evacuate or shelter in place? How are they notified? What routes are used? Are schools, care homes, hospitals, farms, and people without transportation considered? What happens to livestock? What happens during winter storms, wildfire smoke, or road closures?

Emergency plans should account for real communities.

People may not have vehicles. Seniors may need assistance. Hospitals cannot easily evacuate. Farms may have animals. Schools may need reunification plans. People with disabilities may require accessible transportation. Language barriers may exist. Rural residents may have long driveways, private wells, or limited cell service.

A plan that assumes everyone can leave quickly is not a plan for everyone.

Emergency Service Capacity

A data center may require more emergency capacity than the community currently has.

Small or rural fire departments may be volunteer-based. Emergency medical services may already be stretched. Police may cover large areas. Hazardous-material teams may be distant. Specialized battery or high-voltage training may not exist locally. Water supply may be limited. Response times may be long. Mutual aid may be needed.

The public should ask whether local responders have the staffing, training, equipment, water supply, protective gear, site access, communications, and funding needed.

If not, the developer should fund the gap.

A private facility should not create emergency risks that local responders are expected to manage with inadequate tools.

Emergency Communication and Public Notice

During an emergency, people need timely information.

The public should ask how emergency notices will be sent. Will residents receive text alerts, phone calls, sirens, radio notices, social media updates, door-to-door notification, or municipal emergency alerts? Will alerts reach people with disabilities, people without smartphones, people without internet, people who speak other languages, schools, care homes, farms, and remote residents?

Emergency communication should be tested before an emergency.

The public should also know how incidents will be reported afterward. What happened? What substances were involved? What areas were affected? What monitoring occurred? What cleanup is required? What corrective actions will prevent recurrence?

Silence after an incident destroys trust.

Core Questions

Emergency Risk Assessment

What emergencies are possible at the facility?

Has a full emergency risk assessment been completed?

Does it include fire, explosion, battery failure, diesel spill, chemical release, water contamination, cyberattack, grid failure, cooling failure, flood, wildfire, extreme heat, severe weather, evacuation, and security incidents?

Does it include combined emergencies?

Does it include full buildout?

Does it include future phases?

Does it include nearby homes, farms, schools, hospitals, care facilities, roads, waterways, wildlife, and public infrastructure?

Fire and Explosion

What fire risks exist?

What explosion risks exist?

What systems could ignite or fail?

Are batteries, generators, transformers, fuel tanks, electrical rooms, cooling systems, and server rooms assessed separately?

What fire suppression systems are used?

What water supply is required?

Can local fire services provide the required response?

Will firewater or suppression chemicals be contained?

What happens if fire spreads beyond the facility?

Battery Failure

Will batteries be used?

What type?

What capacity?

Where are they located?

What thermal runaway risks exist?

What gases, smoke, toxins, explosion risks, or runoff could result?

What fire suppression methods are required?

Can batteries reignite?

Are local responders trained and equipped?

Will battery incidents trigger public notification?

Diesel, Fuel, and Generators

What fuels are stored on site?

How much fuel is stored?

Where is it stored?

How is it contained?

How are leaks detected?

How often are fuel deliveries made?

What happens if fuel spills?

What happens if generators fail?

What happens if generators run for an extended period?

Could fuel or generator emergencies affect air, soil, water, roads, farms, or homes?

Chemicals and Fire Suppression

What chemicals are stored or used on site?

What coolants, refrigerants, biocides, corrosion inhibitors, cleaning agents, transformer oils, fire suppression chemicals, battery materials, or other substances are present?

What quantities are present?

What happens if they leak, burn, mix, or enter water?

Are safety data sheets available to emergency responders?

Will a plain-language chemical summary be public?

Who is responsible for cleanup?

Water Contamination and Runoff

Could emergency runoff leave the site?

Where would it go?

Can contaminated water be contained?

Are shutoff valves, berms, containment ponds, separators, or emergency storage systems installed?

Can storm drains be isolated?

Could contamination reach groundwater, wetlands, rivers, lakes, ditches, farms, sewer systems, or neighbouring land?

Who tests water after an emergency?

Who notifies downstream users?

Who pays for cleanup?

Cyberattack

What cyberattack scenarios are included in emergency planning?

Could cyberattack affect cooling, power, security, access controls, monitoring, public services, or emergency response?

What happens if ransomware disables systems?

What happens if a cyberattack coincides with a physical emergency?

Can emergency responders access needed site information if digital systems fail?

Will public agencies be notified if their services or data are affected?

Grid Failure and Power Emergency

What happens during a grid failure?
Does the facility switch to backup power?
How long can backup power run?
Will the facility reduce load during grid stress?
Will it have priority power access?
Can it be curtailed?
Will generator operation be reported publicly?
Could generator emissions affect local air during emergencies?
Could fuel deliveries interfere with emergency response?

Extreme Heat and Cooling Failure

What happens during extreme heat?
What happens if cooling systems fail?
Will emergency cooling require more water?
Will it require more power?
Will it require generators?
Will noise, heat rejection, water use, or emissions increase?
Can the facility reduce workload to protect public systems?
Will nearby residents, workers, livestock, crops, or ecosystems face additional heat burden?

Flood, Wildfire, and Severe Weather

Is the site at risk of flooding?
Is it at risk of wildfire?
Is it vulnerable to extreme storms, high winds, hail, lightning, ice, or freezing rain?
Can emergency vehicles access the site during severe weather?
Can nearby residents evacuate if roads are affected?
Are fuel tanks, batteries, electrical systems, and chemicals protected from flood or fire?
Could the facility worsen flood or wildfire risk?
Were future climate conditions assessed?

Evacuation and Shelter-in-Place

What emergencies could require evacuation?
What emergencies could require shelter-in-place?
Who decides?
How are residents notified?
What areas are included?
Are schools, hospitals, care homes, shelters, farms, and people with disabilities included?
Are livestock and farm operations considered?
Are evacuation routes adequate?
What happens if evacuation coincides with wildfire, flood, winter storm, or road closure?

Emergency Services

Can local fire services handle the facility?
Can emergency medical services handle it?
Can police and emergency management handle it?
Is hazardous-materials response available?
Is specialized battery response available?
Is high-voltage response training available?
Is enough water available for firefighting?
Will mutual aid be required?
Who pays for training, equipment, planning, exercises, and additional capacity?

Communication and Reporting

How will the public be notified during an emergency?
Will alerts reach people without smartphones or internet?
Will alerts be accessible to people with disabilities?
Will alerts be available in relevant languages?
Will incident reports be public?
How quickly must incidents be reported?
Who reports to regulators?
Who reports to residents?
Who reports to Indigenous governments, downstream communities, schools, hospitals, farms, and neighbouring jurisdictions where relevant?

Drills and Review

Will emergency drills be required?
How often?
Will local emergency services participate?
Will nearby communities be included?
Will tabletop exercises include combined emergencies?
Will plans be updated after drills, incidents, expansion, equipment changes, or tenant changes?
Will summaries of drills and lessons learned be public?

Red Flags

An emergency planning proposal deserves greater scrutiny when the public hears:
"Emergency plans will be finalized after approval."
"The facility will meet all applicable safety codes."
"Backup systems are designed to prevent failure."
"Battery systems are safe."
"Fuel storage will follow standard procedures."
"Cybersecurity is handled separately."
"Emergency response is the responsibility of local services."
"Incidents are unlikely."

"Security concerns prevent disclosure."
"Fire protection will be reviewed at the building permit stage."
"Mutual aid can be used if needed."

Code compliance is not the same as community preparedness.
An unlikely emergency is still an emergency.
A private risk is not private if public responders must manage it.
Security does not justify hiding public safety impacts.
Mutual aid is not a plan if every nearby community may need help at the same time.

What Communities Should Ask For

Before approval, communities should ask for:
A full emergency risk assessment.
A fire and explosion response plan.
A battery failure and thermal runaway response plan.
A diesel, fuel, and generator emergency plan.
A chemical release and fire suppression response plan.
A contaminated runoff and water protection plan.
A cyberattack and digital emergency plan.
A grid failure and backup power plan.
An extreme heat and cooling failure plan.
A flood, wildfire, and severe weather plan.
An evacuation and shelter-in-place plan.
A public emergency notification plan.
A first responder access and site safety plan.
A local emergency service capacity assessment.
A funding agreement for any additional training, equipment, staffing, water capacity, communications, or planning required.
A mutual aid assessment.
Emergency drills and tabletop exercises before operation begins.
Public reporting requirements for incidents, drills, corrective actions, and plan updates.
Independent review of emergency planning before approval and after major changes.
Clear legal authority to pause operations, restrict systems, require mitigation, or reopen permits if emergency risks are greater than predicted.

The Public Interest Standard

No data center should be approved until emergency planning is complete, reviewed by public authorities, funded, tested, and adequate for the full range of risks the facility creates.

A community should not be asked to accept fire risk, battery risk, diesel risk, chemical risk, cyber risk, water contamination risk, grid risk, heat risk, flood risk, wildfire risk, or evacuation burden without knowing who responds and who pays.

Emergency planning is not paperwork.

It is the difference between a private facility failing privately and a public community being harmed publicly.

If the risk reaches beyond the fence, the plan must reach beyond the fence too.

23 - Conditions, Clawbacks, and Public Remedies

A promise is not protection.

A company may promise jobs, tax revenue, water efficiency, renewable energy, low noise, local hiring, public reporting, waste heat recovery, environmental protection, Indigenous consultation, data sovereignty, privacy safeguards, emergency preparedness, or community benefit.

But if nothing happens when those promises are broken, they were never conditions.

They were marketing.

The public should not ask only:

What has the company promised?

The better question is:

What happens if the promise is not kept?

Can permits be suspended?

Can tax benefits be revoked?

Can water use be reduced?

Can power demand be capped?

Can generator testing be restricted?

Can fines escalate?

Can public subsidies be clawed back?

Can future phases be stopped?

Can operations be limited?

Can the public trigger review?

A data center approval should not be a one-way door. If the project fails to meet the standards used to justify its approval, the public must have remedies.

Conditions Must Be Specific

Approval conditions should be specific enough to enforce.

A condition that says the company will "minimize water use" is weak.

A condition that sets a maximum daily, monthly, seasonal, annual, peak, drought-period, and full-buildout water limit is stronger.

A condition that says the company will "support local jobs" is weak.

A condition that requires a specific number of permanent full-time local jobs, wage standards, reporting, and clawbacks is stronger.

A condition that says noise will be "managed" is weak.

A condition that sets enforceable sound limits by location, time of day, frequency range, generator operation, and expansion phase is stronger.

The public should not accept conditions written in promotional language. Conditions should be measurable, time-bound, independently verifiable, publicly reported, and tied to consequences.

If a condition cannot be measured, it cannot be enforced.

Promises Used to Win Approval Should Become Legal Obligations

If a claim helped justify approval, it should become binding.

If the developer claimed the project would create jobs, that job commitment should be enforceable.

If it claimed low water use, that water use should be capped.

If it claimed renewable power, the renewable commitment should be defined and audited.

If it claimed low noise, full-spectrum noise limits should be imposed.

If it claimed no ratepayer burden, ratepayer protections should be written into the agreement.

If it claimed public benefit, that benefit should be legally required.

A company should not be allowed to make one set of claims to gain approval and then operate under a looser set of obligations after approval.

The public-interest record should become the enforcement record.

Clawbacks

Clawbacks allow the public to recover benefits if promises are not met.

If a data center receives tax incentives, grants, discounted utilities, public infrastructure, land discounts, workforce funding, or other public support, those benefits should be conditional.

Clawbacks should apply when the company fails to meet job targets, local hiring commitments, wage standards, tax revenue projections, water limits, energy commitments, environmental conditions, data sovereignty protections, public reporting obligations, community benefit agreements, decommissioning requirements, or other approval terms.

Clawbacks should also apply if the project is sold, delayed, downsized, abandoned, automated, converted to a different use, or transferred to another owner in ways that undermine the public-interest case used to approve it.

A clawback should not be symbolic.

It should be large enough to recover real public value.

Escalating Penalties

Penalties should increase when violations repeat or worsen.

A first violation may require notice, correction, public reporting, and mitigation. Repeated violations should trigger larger fines, independent audits, operating restrictions, suspension of incentives, denial of future phases, or permit review. Serious violations should allow immediate action.

A company should not be able to treat fines as a cost of doing business.

If violating a condition is cheaper than complying with it, the enforcement system has failed.

Escalating penalties should apply to water overuse, emissions exceedances, noise violations, unauthorized generator testing, unreported outages, monitoring failures, data reporting failures, chemical releases, public complaint failures, privacy violations, unauthorized tenant changes, and other breaches of approval conditions.

Permit Suspension and Operating Restrictions

Some violations require more than fines.

If a facility repeatedly exceeds water limits, regulators should be able to reduce water use.

If it violates noise limits, regulators should be able to restrict equipment operation, generator testing, nighttime activity, or future expansion.

If it exceeds emissions limits, regulators should be able to restrict generator use, require cleaner equipment, or suspend testing.

If it fails to report data, regulators should be able to pause expansion or suspend incentives.

If emergency risks are not corrected, regulators should be able to restrict operations until safety is restored.

If a company cannot operate within the conditions that justified approval, the public should not be forced to tolerate the violation indefinitely.

Permits should be living instruments, not permanent shields.

Future Phases Should Be Conditional

Future phases should not be automatic.

A data center may be approved in phases, but expansion should depend on performance. A company that has failed to meet conditions in Phase One should not receive automatic approval for Phase Two. A company that exceeds water limits, noise limits, power demand, emissions, traffic impacts, or public reporting requirements should not be allowed to expand as though nothing happened.

Future phases should require a compliance review.

Before any expansion, the public should know whether the facility met its original commitments, whether impacts matched predictions, whether complaints were resolved, whether monitoring data is complete, whether public costs increased, and whether any conditions need to be strengthened.

Expansion should be earned through compliance, not assumed through initial approval.

Public Trigger Rights

The public should not have to wait for regulators to act.

Approval conditions should include public trigger rights. These allow residents, Indigenous governments, municipalities, farmers, workers, public agencies, or affected communities to request review when specific conditions occur.

Trigger events may include repeated complaints, monitoring exceedances, water shortages, drought, unexpected noise, generator overuse, emergency incidents, ownership changes, tenant changes, expansion proposals, public subsidy failures, data breaches, ecological impacts, or failure to publish required reports.

A public trigger should not automatically mean the project is stopped. It means the issue must be investigated, reported, and answered.

The public should have a formal path to accountability.

A complaint system without review power is only a suggestion box.

Public Remedies

Public remedies are the tools available when harm occurs.

Remedies may include fines, refunds, tax incentive cancellation, subsidy clawbacks, mandatory mitigation, independent audits, public apologies, restoration orders, water reductions, generator restrictions, lighting changes, sound barriers, equipment replacement, habitat restoration, road repairs, emergency service funding, data deletion, privacy remedies, compensation, permit amendments, suspension of future phases, or decommissioning orders.

The remedy should match the harm.

If a company overuses water, a fine may not be enough. The water use may need to be reduced.

If sound levels exceed limits, a report may not be enough. Equipment may need to be modified.

If tax incentives were granted for jobs that never arrived, the public should recover the benefit.

If public data is misused, the system may need to be suspended.

If habitat is damaged, restoration may be required.

If infrastructure costs were shifted to ratepayers, cost recovery may be necessary.

Public remedies should repair harm, prevent recurrence, and restore public trust where possible.

Conditions Should Survive Sale or Restructuring

A data center may be sold, refinanced, merged, transferred, restructured, or placed under new ownership.

Approval conditions should not disappear when ownership changes.

All obligations should run with the land, the facility, the permits, the utility agreements, the water licences, the tax agreements, and the public subsidy arrangements. New owners should inherit the conditions. Parent companies should remain responsible where guarantees were required. Public agencies should be notified before any ownership, operator, or tenant change that could affect compliance.

A company should not be able to escape conditions by selling the asset.

If the public obligations made the project acceptable, they must remain attached to the project.

Reporting Failures Are Violations

A failure to report should be treated as a violation in itself.

If water use, power demand, emissions, sound levels, generator testing, incidents, complaints, jobs, subsidies, ownership changes, tenant changes, or public benefits must be reported, then late reporting, incomplete reporting, inaccurate reporting, or refusal to report should trigger penalties.

The public should not have to prove harm before transparency rules are enforced.

Transparency is itself a condition of approval.

If the company fails to provide the data needed to assess compliance, then the public should presume non-compliance until the record is corrected.

Independent Enforcement

Enforcement should not depend on the company's goodwill.

Regulators and public authorities need staff, authority, funding, technical expertise, access to data, inspection rights, and legal power to enforce conditions. If the project is complex, the developer should fund independent monitoring and enforcement without controlling the monitors or inspectors.

The public should ask who enforces each condition.

Municipality?

Province or state?

Federal regulator?

Utility regulator?

Water authority?

Environmental agency?

Privacy commissioner?

Public health authority?

Indigenous government?

Independent auditor?

If no one is clearly responsible, the condition may be meaningless.

Every condition should have an enforcement owner.

Enforcement Must Be Public

The public should be able to see whether enforcement happened.

If a violation occurs, the public should know what was violated, when it occurred, how it was detected, what harm resulted, what corrective action was required, what penalty was imposed, whether the company complied, and whether the violation affects future approvals or subsidies.

Enforcement hidden from public view does not build trust.

Public enforcement records should be searchable, archived, and plain-language. Repeat violations should be easy to identify. Settlements should not erase the public record. Confidentiality should not hide failures involving public resources, public subsidies, public infrastructure, public health, public data, or environmental harm.

Core Questions

Conditions

What conditions are attached to approval?

Are they specific?

Are they measurable?

Are they time-bound?

Are they independently verifiable?

Are they publicly reported?

Are they legally enforceable?

Which promises made during the approval process became binding conditions?

Which promises remain voluntary or promotional?
Who enforces each condition?

Clawbacks

What public subsidies are subject to clawback?
What tax incentives are subject to clawback?
What grants, loans, discounts, land benefits, utility rates, or infrastructure supports are subject to clawback?
What triggers clawback?
Job shortfalls?
Local hiring failures?
Water overuse?
Power demand increases?
Environmental violations?
Failure to report?
Ownership change?
Tenant change?
Sale?
Abandonment?
Failure to deliver community benefits?
How much can the public recover?
How quickly can recovery occur?

Permits and Operating Limits

Can permits be suspended?
Can permits be amended?
Can future phases be denied?
Can water use be reduced?
Can power demand be capped?
Can generator testing be restricted?
Can operating hours be limited?
Can noisy equipment be restricted at night?
Can lighting be reduced?
Can emissions be limited?
Can cooling methods be changed or restricted?
Can the facility be required to install additional mitigation?

Escalating Penalties

Do fines increase for repeated violations?
Are penalties large enough to change behaviour?
Are penalties automatic for certain violations?
Do serious violations trigger immediate action?

Can violations lead to suspension of tax benefits?

Can violations lead to loss of subsidies?

Can violations lead to permit review?

Can repeated violations trigger independent management, operating restrictions, or decommissioning requirements?

Public Trigger Rights

Can residents request review?

Can Indigenous governments request review?

Can municipalities request review?

Can farmers or landowners request review?

Can public agencies request review?

Can a certain number of complaints trigger investigation?

Can monitoring exceedances trigger public review?

Can drought, outages, emergency incidents, ownership changes, tenant changes, or data breaches trigger review?

Is the response deadline defined?

Are review outcomes public?

Reporting and Transparency

What must be reported?

Water use?

Power demand?

Generator testing?

Emissions?

Noise?

Heat?

Discharge?

Incidents?

Complaints?

Jobs?

Subsidies?

Ownership changes?

Tenant changes?

Public benefits?

What happens if reporting is late, incomplete, inaccurate, or withheld?

Are reports independently audited?

Are enforcement actions public?

Public Remedies

What remedies are available if harm occurs?

Can the public recover subsidies?

Can the public recover infrastructure costs?
Can affected residents receive compensation?
Can farmers receive compensation for livestock, crop, water, or land impacts?
Can habitat restoration be required?
Can road repairs be required?
Can emergency service funding be required?
Can privacy violations trigger data deletion, system suspension, or public notice?
Can public agencies terminate contracts?
Can the company be required to fund independent health, environmental, or technical reviews?

Sale, Transfer, and Restructuring

Do all conditions survive sale?
Do all conditions survive merger?
Do all conditions survive bankruptcy?
Do all conditions survive transfer to a new operator?
Do all conditions bind future tenants?
Do public subsidies transfer automatically?
Do clawbacks apply if the facility is sold?
Is public notice required before ownership, operator, or tenant changes?
Can approval be reopened if ownership or use changes materially?

Enforcement Authority

Which agency enforces water conditions?
Which agency enforces power conditions?
Which agency enforces emissions conditions?
Which agency enforces noise and light conditions?
Which agency enforces wildlife and habitat conditions?
Which agency enforces tax and subsidy conditions?
Which agency enforces privacy and data conditions?
Which agency enforces emergency planning conditions?
Do agencies have enough staff and funding?
Does the developer fund enforcement capacity?
Can inspectors access the site?
Can regulators access raw data?

Future Phases

Can future phases proceed automatically?
Is compliance review required before expansion?
Can future phases be denied because of past violations?
Will expansion require updated monitoring, public consultation, and cumulative impact review?
Do unresolved complaints block expansion?
Do unpaid penalties block expansion?

Do failed promises block expansion?
Can new conditions be added before future phases?

Red Flags

A conditions, clawbacks, or public remedies proposal deserves greater scrutiny when the public hears:

"Conditions will be finalized later."
"The company is committed to being a good neighbour."
"Existing enforcement processes are sufficient."
"Clawbacks are not necessary."
"Future phases are part of the original approval."
"Violations will be handled through normal regulatory channels."
"Public complaints will be reviewed."
"Fines are available under existing law."
"The agreement is commercially confidential."
"Ownership changes will not affect obligations."
"Reporting will be provided annually."

Goodwill is not a condition.
A fine is not a remedy if it is cheaper than compliance.
A complaint process is not review power.
A confidential agreement is not public accountability.
A promise without consequence is not a public safeguard.

What Communities Should Ask For

Before approval, communities should ask for:
A complete list of legally binding approval conditions.
A table linking each public promise to an enforceable obligation.
Specific limits for water, power, noise, emissions, heat, discharge, generator testing, lighting, traffic, and expansion where relevant.
A subsidy clawback framework.
Tax incentive cancellation provisions.
Escalating penalties for repeated or serious violations.
Permit suspension and amendment powers.
Operating restriction powers.
Future phase compliance review requirements.
Public trigger rights.
Complaint escalation rules.
Independent auditing requirements.
Public enforcement reporting.
Clear assignment of enforcement responsibility to specific agencies.
Funding for monitoring, inspection, legal action, public reporting, and enforcement.

Parent-company guarantees where local entities have limited assets.

Financial security, bonds, or reserve funds where public risk exists.

Conditions that survive sale, merger, restructuring, bankruptcy, tenant change, and operator change.

Clear remedies for residents, farmers, Indigenous governments, public agencies, ratepayers, and affected communities where harm occurs.

The Public Interest Standard

No data center should be approved unless its promises are enforceable, its subsidies are recoverable, its violations carry consequences, and the public has a path to trigger review when harm occurs.

A community should not be asked to accept vague commitments in exchange for real land, real water, real power, real infrastructure, real risk, and real public cost.

If the company promises benefits, those benefits should be binding.

If the company causes harm, remedies should be available.

If the company breaks conditions, consequences should follow.

And if the public is expected to live with the project, the public must have more than trust.

It must have power.

24 - Community Benefit Agreements

A data center can create public burdens even when it is privately owned.

It may use public roads, public water, public grid capacity, public emergency services, public staff time, public land-use authority, public tax incentives, public infrastructure, public trust, and public patience. It may affect homes, farms, ecosystems, ratepayers, workers, Indigenous rights, local planning, and future community development.

If the community is expected to host those burdens, the community should receive more than promises.

It should receive enforceable benefits.

A Community Benefit Agreement is one way to make that happen.

The public should not ask only:

What does the company say the community will gain?

The better question is:

What benefits are legally guaranteed, who receives them, who measures them, who enforces them, and what happens if they are not delivered?

A community benefit should not be a donation, a sponsorship, a photo opportunity, or a voluntary gesture. It should be a binding public-interest return connected to the real impacts, costs, and risks of the project.

If a data center is asking a community to share its land, water, electricity, infrastructure, roads, air, silence, and future capacity, then the project should return measurable value to that community.

Benefits Should Match the Burden

A Community Benefit Agreement should be designed around the specific project and the specific community.

A facility that uses significant electricity should not offer only a scholarship fund while leaving ratepayers exposed. A facility that produces waste heat should not waste that heat while public buildings pay to stay warm. A facility that requires road upgrades should not leave road maintenance to taxpayers. A facility that affects farms should not ignore agricultural impacts. A facility that increases emergency risk should not leave fire departments underfunded. A facility that receives tax breaks should not offer vague promises in return.

Benefits should respond to burdens.

If the burden is water, the benefit may include water restoration, conservation funding, watershed monitoring, drought resilience, public water infrastructure, or water-use offsets.

If the burden is electricity, the benefit may include local renewable generation, storage, grid upgrades that serve residents, ratepayer protections, energy-efficiency funding, or public building retrofits.

If the burden is heat, the benefit may include waste heat recovery, district heating, greenhouse heating, public facility heating, or community energy systems.

If the burden is emergency risk, the benefit may include fire equipment, emergency training, hazardous-material response capacity, public alert systems, or dedicated funding.

If the burden is land, the benefit may include habitat restoration, farmland protection, public trails, conservation easements, buffers, tree planting, or ecosystem repair.

A benefit that does not respond to the burden may be public relations, not public value.

Local Hiring and Training

Job promises should be turned into enforceable commitments.

A Community Benefit Agreement should specify how many local workers will be hired, what kinds of jobs will be created, what wages will be paid, what training will be provided, and how local residents will be prepared to compete for those jobs.

Local hiring should include construction jobs, permanent jobs, apprenticeships, technical training, maintenance roles, security positions, operations work, and vendor contracts where possible.

The agreement should also address Indigenous hiring, youth training, underemployed workers, displaced workers, people with disabilities, women in trades and technology, and workers from communities directly affected by the project.

Training should begin before construction, not after specialized jobs have already been filled by outside workers.

A project should not claim local economic benefit if local people are not given a real pathway into the work.

Local Procurement and Small Business Access

A data center may spend large amounts of money during construction and operation.

The public should ask how much of that spending will stay in the region.

A Community Benefit Agreement can require local procurement targets, Indigenous procurement targets, small business access, transparent bidding, unbundled contracts, supplier fairs, technical assistance for local firms, and public reporting on where money is spent.

Large companies often rely on large existing vendors. Without enforceable procurement rules, local businesses may see little benefit from a project promoted in their name.

If public resources support the project, local businesses should have a fair chance to participate.

Public Broadband and Digital Access

A data center may bring fiber routes, network capacity, and digital infrastructure into a region.

The public should ask whether the community will benefit from that infrastructure.

If a project requires new fiber, communications systems, or network upgrades, a Community Benefit Agreement could require public broadband improvements, affordable internet access, school connectivity, library connectivity, rural broadband expansion, community Wi-Fi, digital literacy programs, or support for local public-interest technology.

A community should not watch massive digital infrastructure arrive beside it while residents, schools, farms, libraries, and small businesses still struggle with poor connectivity.

If the facility is part of the digital economy, the community should not remain on the wrong side of the digital divide.

District Heating and Waste Heat Use

Data centers produce heat.

That heat should not automatically be wasted.

A Community Benefit Agreement can require a waste heat recovery study, district heating planning, connection points for future heat recovery, or direct use of waste heat for public buildings, greenhouses, food production, social housing, recreation centres, schools, hospitals, libraries, municipal buildings, emergency shelters, or seniors' facilities.

Not every site will be suitable for heat reuse, but the question should be asked early.

If the community is helping provide the electricity, land, water, and infrastructure that make the facility possible, then the community should receive first consideration for any practical use of the heat it produces.

Waste heat should not be treated as a private inconvenience when it could become a public asset.

Water Offsets and Watershed Benefits

If a data center uses water or affects water systems, the community benefit should include water protection.

That may include watershed restoration, wetland repair, leak reduction in municipal systems, agricultural water efficiency, public water monitoring, aquifer studies, drought planning, stormwater improvements, riparian buffers, water reuse infrastructure, or funding for local water conservation.

Water offsets should be real, local, measurable, and additional. They should not be paper credits or distant projects that do nothing for the affected watershed.

If the project increases water stress, the benefit agreement should help reduce water stress.

If it affects a watershed, the benefit should return value to that watershed.

Environmental Restoration

A data center may affect land, habitat, wildlife corridors, wetlands, forests, grasslands, soil, pollinators, birds, bats, amphibians, aquatic life, and agricultural systems.

Community benefits should include environmental restoration where impacts occur.

That may include native planting, tree canopy, wetland restoration, habitat corridors, pollinator habitat, streambank repair, soil restoration, invasive species control, wildlife crossings, dark-sky lighting, conservation easements, farmland protection, or long-term ecological monitoring.

Environmental restoration should not be vague beautification.

It should be scientifically grounded, locally appropriate, maintained over time, and independently monitored.

A row of ornamental shrubs is not a habitat plan.

Emergency Service Funding

If a data center creates specialized emergency risks, the developer should help pay for emergency readiness.

A Community Benefit Agreement can fund fire equipment, hazardous-material training, battery response training, high-voltage training, emergency communication systems, public alert tools, water supply improvements, evacuation planning, emergency drills, protective gear, mutual aid capacity, and staffing where needed.

Emergency service funding should be based on the risk created by the project, not on what the municipality can afford after the fact.

A private facility should not create a public emergency burden and then leave local responders to pass the hat.

Public Reporting and Transparency

A Community Benefit Agreement should include public reporting requirements.

The community should be able to see whether benefits are being delivered. Reporting should include local hiring, wages, training, procurement, subsidies, public infrastructure, water use, power use, environmental restoration, emergency service funding, complaints, monitoring results, and compliance with agreement terms.

Reports should be public, regular, plain-language, archived, and independently verified where necessary.

A benefit that cannot be seen, measured, or audited may not be a benefit.

Transparency should be part of the bargain.

Community Governance

A Community Benefit Agreement should not be written only by the developer and government behind closed doors.

Affected communities should have a role in shaping the agreement. That may include residents, Indigenous governments, farmers, workers, local businesses, schools, health providers, environmental groups, youth, seniors, disability advocates, emergency responders, and neighbouring municipalities.

The agreement may create a community oversight committee, public reporting forum, annual review meeting, or independent benefit administrator.

Community governance matters because needs change.

A benefit package negotiated at the beginning of a project may need adjustment as impacts become clearer, phases expand, tenants change, or public conditions shift.

The community should have a continuing voice, not only a consultation window.

Indigenous Community Benefits and Rights

Community Benefit Agreements must not be used as a substitute for Indigenous rights, treaty obligations, consultation, consent, or Indigenous jurisdiction.

Where Indigenous governments, Nations, lands, waters, rights, data, cultural sites, harvesting areas, or traditional territories may be affected, benefit agreements should be negotiated directly with Indigenous governments according to their own laws, protocols, priorities, and decision-making processes.

Benefits may include Indigenous employment, procurement, training, equity participation, water protection, land restoration, cultural protection, data governance, environmental monitoring, revenue sharing, guardians programs, or other Nation-defined priorities.

But benefits should not be used to buy silence or bypass rights.

A benefit agreement is not consent unless the rights-holding Indigenous government says it is.

Enforceability

Community benefits should be legally enforceable.

The agreement should define each benefit, timeline, funding amount, recipient, measurement method, reporting requirement, enforcement mechanism, and consequence for failure.

If the company misses hiring targets, what happens?
If training funds are not delivered, what happens?
If waste heat recovery is not built, what happens?
If public broadband commitments are delayed, what happens?
If environmental restoration fails, what happens?
If emergency service funding is not paid, what happens?
If ownership changes, do the obligations survive?

A Community Benefit Agreement should include clawbacks, penalties, escrow funds, bonds, letters of credit, parent-company guarantees, public reporting, independent audits, and clear legal standing for enforcement.

A voluntary benefit is not enough when the burdens are mandatory.

Benefits Should Survive Sale and Expansion

Data centers can change owners, tenants, operators, and uses.

Community benefit obligations should survive those changes.

If the facility is sold, the new owner should inherit the agreement. If the operator changes, obligations should continue. If tenants change, benefits should remain. If the facility expands, benefits should expand too. If the project receives more public support, the community return should be reconsidered.

A company should not be able to escape community obligations by selling the asset after the public has already provided land-use approval, infrastructure, water, grid access, or tax incentives.

Benefits should run with the project, not the press conference.

Core Questions

Agreement Structure

Will there be a Community Benefit Agreement?

Who will negotiate it?

Who will be legally bound by it?

Will the agreement include the applicant, landowner, building owner, operator, parent company, tenants, subsidy recipients, and future owners where appropriate?

Will the agreement be public?

Will it be legally enforceable?

Who has standing to enforce it?

Will obligations survive sale, merger, restructuring, bankruptcy, tenant change, operator change, and future expansion?

Local Hiring and Training

How many local construction jobs are guaranteed?

How many permanent local jobs are guaranteed?

What wages and benefits are required?

Will apprenticeships be funded?

Will technical training be provided?

Will local colleges, trade schools, unions, Indigenous governments, workforce agencies, or schools be involved?

Will hiring include affected communities, Indigenous workers, youth, women in trades and technology, people with disabilities, and underemployed workers?

Will hiring data be public?

What happens if targets are missed?

Local Procurement

What percentage of procurement will go to local businesses?

What percentage will go to Indigenous businesses?

Will small businesses be able to bid?

Will contracts be structured so local firms can participate?

Will procurement opportunities be advertised publicly?

Will supplier support be provided?

Will procurement results be publicly reported?

What happens if procurement targets are missed?

Public Broadband and Digital Access

Will the project improve public broadband?

Will schools, libraries, public facilities, rural areas, farms, low-income households, or small businesses receive improved access?

Will fiber routes include public access or community benefit capacity?

Will affordable internet programs be funded?

Will digital literacy programs be supported?

Will public broadband commitments be enforceable?

Will the community benefit from digital infrastructure, or only host it?

District Heating and Waste Heat

Will waste heat recovery be required?

Has a feasibility study been completed?

Could public buildings be heated?

Could schools, hospitals, recreation centres, libraries, municipal buildings, seniors' homes, social housing, shelters, greenhouses, food production, or industrial users benefit?

Will connection points be built even if immediate reuse is not possible?

Who pays for heat recovery infrastructure?

Who owns it?

Will recovered heat be offered at a public-benefit rate?

What happens if the company refuses future connection?

Water Offsets and Watershed Benefits

Will the project fund water conservation?

Will it fund leak reduction?

Will it fund watershed restoration?

Will it fund wetland restoration?

Will it fund drought resilience?

Will it fund public water monitoring?

Will it fund agricultural water efficiency?

Will offsets occur in the affected watershed?

Are offsets measurable, additional, local, and enforceable?

Who verifies the water benefit?

Environmental Restoration

What restoration will be required?

Will habitat corridors be protected or restored?

Will wetlands be restored?

Will native vegetation be planted?

Will pollinator habitat be created?

Will tree canopy be expanded?

Will soil health be restored?

Will invasive species be managed?

Will wildlife crossings or dark corridors be created?

Will restoration be monitored over time?

Who maintains restoration areas?

What happens if restoration fails?

Emergency Services

What emergency service funding will be provided?

Will fire departments receive equipment?

Will responders receive training for battery fires, high-voltage systems, fuel spills, chemical releases, and data center emergencies?

Will public alert systems be funded?

Will emergency drills be funded?

Will hazardous-material response capacity be improved?

Will water supply or fire-flow capacity be upgraded?
Will funding continue for the life of the risk?
What happens if emergency service needs increase?

Public Reporting

What benefits will be reported?
How often?
Will reports include jobs, wages, procurement, training, public broadband, waste heat, water offsets, environmental restoration, emergency service funding, subsidies, monitoring, complaints, and compliance?
Will reports be public?
Will data be independently audited?
Will the public be able to compare promised benefits with delivered benefits?
Will annual public meetings be required?

Community Governance

Will a community oversight committee be created?
Who will sit on it?
Will residents, Indigenous governments, farmers, workers, local businesses, youth, seniors, disability advocates, environmental groups, emergency responders, and public agencies be represented where relevant?
Will the committee have access to data?
Can it recommend enforcement?
Can it trigger review?
Will it have funding and independence?
Will meetings and reports be public?

Enforcement

What happens if benefits are not delivered?
Can payments be withheld?
Can subsidies be clawed back?
Can tax incentives be cancelled?
Can future phases be paused?
Can penalties be imposed?
Can the public sue to enforce the agreement?
Are funds held in escrow?
Are bonds or letters of credit required?
Does the parent company guarantee the obligations?
Can the agreement be amended without public approval?

Red Flags

A Community Benefit Agreement proposal deserves greater scrutiny when the public hears: "The company is committed to being a good neighbour."

"Community benefits will be developed later."
"Local hiring will be encouraged."
"Training partnerships may be explored."
"Waste heat recovery could be considered in the future."
"The project will support regional growth."
"Benefits will be provided voluntarily."
"Details are still being negotiated."
"The agreement is commercially confidential."
"Public reporting is not necessary."
"The company has a strong record of community investment."

Goodwill is not a benefit agreement.
Encouragement is not a hiring target.
Exploration is not a commitment.
A voluntary donation is not a public return.
A confidential community benefit is not community accountability.

What Communities Should Ask For

Before approval, communities should ask for:
A legally binding Community Benefit Agreement.
Public disclosure of the agreement before final approval.
Specific local hiring, wage, training, apprenticeship, and procurement commitments.
Indigenous hiring, procurement, and benefit provisions where appropriate and rights-holders agree.
Public broadband and digital access commitments where digital infrastructure is expanded.
Waste heat recovery and district heating assessments, with enforceable commitments where feasible.
Water offsets and watershed benefit commitments where water systems are affected.
Environmental restoration and long-term maintenance commitments.
Emergency service funding commitments.
Public reporting requirements.
Independent auditing.
Community oversight.
Clawbacks and penalties for non-compliance.
Escrow funds, bonds, letters of credit, or parent-company guarantees.
Requirements that benefits survive sale, restructuring, operator change, tenant change, and expansion.
Review points that allow benefits to be strengthened if impacts grow or public support increases.

The Public Interest Standard

No data center should receive public approval, public infrastructure, public subsidies, public resources, or public tolerance without enforceable public return.

A Community Benefit Agreement should not be a ribbon-cutting accessory.

It should be the written answer to a basic question:

If this community is being asked to host the burden, what does the community receive in return?

Not as charity.

Not as branding.

Not as vague future partnership.

As a binding condition of development.

A data center that consumes from the public should give back to the public in ways that are real, measurable, local, durable, and enforceable.

Addendum A

Artificial Intelligence

Not every data center is an artificial intelligence facility.

That distinction matters.

Some data centers support cloud storage, business systems, streaming, financial services, public records, research, communications, health systems, education platforms, or ordinary enterprise computing. Others are built or adapted to support high-density artificial intelligence workloads, including model training, model fine-tuning, inference, data processing, synthetic data generation, surveillance analytics, automation tools, and large-scale commercial AI services.

The public should be careful not to collapse every data center conversation into an AI conversation.

That can allow industry and governments to deflect legitimate concerns by saying, "This is not only about AI," or "Not all data centers are AI data centers." Those statements may be true. But they do not end the public-interest inquiry.

The better framing is this:

Data centers are the physical infrastructure of the digital economy.

Artificial intelligence is one of the forces rapidly increasing demand for that infrastructure.

The two issues overlap, but they are not identical.

This handbook focuses on the land, water, power, sound, heat, emissions, public cost, sovereignty, privacy, and accountability questions that should apply to data center development regardless of whether a facility is AI-focused. This addendum addresses the additional questions that arise when a data center supports artificial intelligence.

AI Is Not Only a Computing Question

The public debate around artificial intelligence often focuses on future regulation, model safety, copyright, jobs, misinformation, automation, bias, surveillance, or existential risk.

Those are important questions.

But for communities facing data center development, AI also raises a more immediate question:

What data is being used, who controls it, where did it come from, and what can it be used to build?

Governments are racing to legislate AI controls, but the technology is already moving faster than the law. By the time legislation catches up to one generation of AI systems, the next generation may already be trained, deployed, integrated, and normalized.

If communities want to have an immediate effect on AI and its future iterations, they should focus not only on the models themselves, but on access to data — especially personal data, public data, biometric data, health data, student data, location data, behavioural data, Indigenous data, creative work, and data collected through essential services.

Without data, AI systems cannot be trained, refined, personalized, targeted, evaluated, or expanded in the same way.

Data is not just an input.

Data is the soil AI grows from.

The Data Center as AI Infrastructure

A data center may support AI in several ways.

It may train large models. It may fine-tune existing models. It may run inference services. It may process datasets. It may store training material. It may host AI tools used by governments, corporations, schools, hospitals, police, courts, advertisers, insurers, employers, or public agencies. It may provide the computing power needed to analyze video, audio, images, text, location data, health data, education records, public-service records, or consumer behaviour.

The facility may not be labelled an "AI data center."

It may be called a cloud region, technology campus, digital infrastructure project, advanced computing site, hyperscale facility, enterprise data center, research facility, innovation hub, or high-performance computing project.

The public should ask what the facility is capable of supporting, not only how it is branded.

If a data center is designed for high power density, advanced cooling, large-scale GPU clusters, AI accelerators, high-speed networking, or rapid expansion, then AI-related uses should be part of the public-interest review.

Training, Inference, and Demand

AI systems create different infrastructure demands depending on how they are used.

Training large models can require enormous computing power for concentrated periods. Fine-tuning may require smaller but still significant workloads. Inference — the use of AI systems after training — can create continuous demand as millions of people, businesses, devices, platforms, governments, and automated systems send requests to models.

The public should ask whether the facility will support training, inference, or both.

This matters because different AI workloads may create different electricity demand, cooling demand, water demand, heat output, hardware turnover, backup needs, and operational patterns. A

facility built for AI may need more power density, more advanced cooling, more frequent equipment replacement, and more grid capacity than a traditional data storage facility.

A proposal should not be allowed to present itself as ordinary digital infrastructure if its design is driven by AI-scale demand.

AI and Personal Data

Personal data is one of the central issues in AI governance.

AI systems may be trained, fine-tuned, tested, prompted, evaluated, personalized, or deployed using information about real people. That may include names, faces, voices, writing, images, health records, education records, social media activity, browsing behaviour, location data, purchases, financial records, employment records, biometric identifiers, public-service records, communications, and metadata.

The public should ask whether the data center will store or process personal data used for AI systems.

Will personal data be used for training?

Will it be used for fine-tuning?

Will it be used for inference?

Will prompts be stored?

Will user interactions be logged?

Will metadata be retained?

Will data be used to improve models?

Will people be able to opt out?

Will deletion requests actually remove data from training pipelines, backups, logs, and derived systems?

If personal data is being used to build AI systems, the public should not be told that the issue is only technical.

It is a rights issue.

Public Data and AI

Public-sector data is especially sensitive.

Governments collect information because they have public authority. People often cannot refuse to provide it. Health systems, schools, courts, police, social services, public housing agencies, utilities, licensing bodies, tax authorities, immigration systems, and emergency services all collect information that may be deeply personal, sensitive, or life-altering.

If that data is used for AI, the risks are significant.

Public data may be used to automate decisions, predict behaviour, identify risk, flag fraud, allocate services, recommend policing action, score students, triage patients, evaluate benefits, prioritize inspections, or influence court, immigration, housing, employment, health, or education outcomes.

The public should ask whether public-sector data hosted or processed in the facility can be used for AI training, AI testing, automated decision-making, predictive analytics, profiling, or secondary commercial use.

Data collected for a public service should not silently become raw material for AI systems.

Consent to receive health care, attend school, apply for benefits, pay taxes, report a crime, use a library, access utilities, or interact with government is not consent to train or operate AI.

AI, Surveillance, and Public Power

AI can make surveillance more scalable.

A camera network becomes more powerful when paired with facial recognition, object detection, gait analysis, licence plate recognition, behavioural prediction, crowd analysis, or automated alert systems. Public records become more powerful when linked and analyzed. School platforms become more powerful when used to score behaviour or predict risk. Policing databases become more powerful when used to forecast people or places. Immigration systems become more powerful when automated risk tools are added.

A data center may provide the storage and computing power that makes these systems possible.

The public should ask whether the facility will support AI systems used in policing, immigration, corrections, border control, public safety, schools, smart cities, welfare systems, housing, courts, or public health.

AI infrastructure should not be treated as neutral when it can deepen surveillance, automate suspicion, and expand state or corporate power over people who may never know they are being analyzed.

AI Bias and Historical Data

AI systems learn from data.

If the data reflects historical inequality, institutional bias, over-policing, under-service, discrimination, poverty, exclusion, racial profiling, disability discrimination, gender bias, colonial systems, or unequal access to public services, AI systems may reproduce or amplify those patterns.

This is especially important when AI is used in public systems.

A model trained on biased policing data may predict crime where policing was historically concentrated. A model trained on unequal health data may underserve people already neglected by the system. A model trained on school discipline records may reproduce patterns of discrimination. A model trained on social service data may treat poverty as risk. A model trained on court data may treat past injustice as neutral evidence.

The public should ask not only whether an AI system is accurate.

Accurate according to what data?

Accurate for whom?

Accurate at whose expense?

AI governance must include scrutiny of the datasets, not only the model.

Copyright, Creative Work, and Cultural Data

AI systems may be trained on books, art, music, journalism, photographs, films, websites, academic work, software, social posts, and other creative or cultural material.

A data center that supports AI may be processing or storing datasets that include copyrighted work, personal expression, cultural knowledge, Indigenous knowledge, community archives, public records, or materials scraped from the internet without meaningful consent.

The public should ask whether the facility will support AI systems trained on copyrighted, scraped, personal, cultural, or Indigenous materials.

Will creators be compensated?

Was consent obtained?

Can works be removed?

Are Indigenous cultural materials protected?

Are children's images, schoolwork, social posts, or personal writings included?

Are public institutions contributing datasets to AI developers?

AI should not be allowed to convert the work, lives, and cultures of people into private infrastructure without scrutiny.

AI and Indigenous Data Sovereignty

Indigenous data sovereignty is especially important in AI.

AI systems may process data about Indigenous lands, waters, languages, health, children, governance, traditional knowledge, sacred sites, harvesting, culture, ancestry, membership, environmental observations, or historical records.

That data must not be extracted, trained on, commercialized, or analyzed without Indigenous authority and governance.

The public should ask whether any AI systems supported by the facility will use Indigenous data or affect Indigenous rights, lands, waters, knowledge, or governance.

If so, Indigenous governments must determine what is permitted according to their own laws, protocols, consent standards, and data governance principles.

AI should not become a new extraction industry built from Indigenous knowledge and public infrastructure.

AI and Environmental Demand

AI is not weightless.

AI workloads can drive demand for more servers, more electricity, more cooling, more water, more land, more backup systems, more transmission infrastructure, more batteries, more hardware, and more rapid equipment replacement.

A facility built to support AI may carry larger physical impacts than a conventional data center. Higher-density computing can increase heat and cooling demands. Rapid model development can increase hardware turnover. Continuous inference demand can increase baseline power use. Competition among AI companies can pressure governments to approve infrastructure quickly.

The public should ask whether AI workloads are driving the scale of the facility.

If the answer is yes, then the AI use should be part of the environmental and public-cost review.

A community should not be asked to absorb AI's physical footprint while being told the AI debate belongs somewhere else.

AI Regulation Is Not Enough

Governments may pass AI laws, standards, codes of conduct, procurement rules, risk frameworks, or transparency requirements.

Those may help, but they may not be enough.

AI regulation often comes after systems are already built. It may rely on company disclosure. It may be limited by trade secrecy. It may exempt certain systems. It may struggle to keep pace with technical change. It may regulate outputs while leaving data extraction, infrastructure buildout, and public-sector dependency insufficiently addressed.

Communities do not have to wait for perfect AI legislation to ask immediate questions.

They can ask:

What data will this facility process?

Will personal data be used for AI?

Will public data be used for AI?

Will Indigenous data be used for AI?

Will copyrighted or scraped data be used for AI?

Will AI systems supported here be used in public decisions?

Will the facility support surveillance, profiling, or predictive analytics?

Will data be retained, reused, or sold?

Can people opt out?

Can data be deleted?

Can the public audit the use?

These questions can be asked now.

Data Access as the Immediate Point of Control

If AI systems depend on data, then data access is a powerful point of public control.

Communities and governments can act immediately by setting rules on what data may be collected, stored, processed, linked, retained, transferred, sold, or used for AI.

They can prohibit the use of public-sector data for AI training without explicit approval. They can restrict secondary use. They can require data minimization. They can require deletion. They can protect children's data. They can prohibit biometric surveillance. They can require Indigenous data governance. They can require public AI registers. They can require impact assessments before public agencies use AI. They can require human appeal for automated decisions. They can prohibit vendors from using public data for product development. They can require local control of encryption keys. They can require public reporting of AI-related uses.

The most immediate AI question may not be how to regulate a model after it exists.

It may be how to control the data before it becomes part of the model.

Without access to data, many AI systems cannot grow in the same way.

Core Questions

AI Use

Will the facility support artificial intelligence workloads?

Will it support AI training?

Will it support AI fine-tuning?

Will it support AI inference?

Will it support high-performance computing, GPU clusters, AI accelerators, or high-density racks?

Will AI-related uses be disclosed?

Will AI uses be permitted, prohibited, or limited through approval conditions?

Can the facility shift to AI workloads later without public review?

Data Sources

What data will be used by AI systems supported by the facility?

Will personal data be used?

Will public-sector data be used?

Will health data be used?

Will education or children's data be used?

Will court, policing, corrections, immigration, or social service data be used?

Will biometric data be used?

Will location data be used?

Will Indigenous data or traditional knowledge be used?

Will copyrighted or scraped creative work be used?

Will user prompts, interactions, metadata, or logs be retained or used?

Consent and Control

Was consent obtained for AI use?

Can people opt out?

Can public agencies prohibit AI training on their data?

Can Indigenous governments control AI use of Indigenous data?

Can creators remove their work?

Can children's data be excluded?

Can sensitive data be deleted from AI pipelines?

Does deletion apply to backups, logs, derived datasets, embeddings, fine-tuned models, and model outputs where feasible?

Who verifies compliance?

Public-Sector AI

Will the facility support AI used by governments or public agencies?

Will AI systems affect decisions about health care, education, policing, courts, corrections, immigration, housing, benefits, child welfare, utilities, transportation, taxation, or emergency services?

Will people know when AI affects a decision?
Can they appeal to a human?
Are public AI systems listed in a public register?
Are impact assessments public?
Are audits public?
Can harmful systems be suspended?

Surveillance and Biometrics

Will the facility support facial recognition?
Will it support licence plate recognition?
Will it support public camera analytics?
Will it support smart-city surveillance?
Will it support predictive policing?
Will it support immigration enforcement?
Will it support crowd monitoring, protest monitoring, behavioural analysis, or social media monitoring?
Are any surveillance or biometric uses prohibited?
Who approves new surveillance uses?

Bias, Accuracy, and Harm

What datasets are used to train or evaluate AI systems?
Have datasets been assessed for bias?
Have systems been tested across affected populations?
Are errors publicly reported?
Who is harmed by false positives?
Who is harmed by false negatives?
Are decisions explainable?
Can people challenge or correct underlying data?
Can systems be stopped if harm is identified?

Environmental and Infrastructure Demand

How much power demand is tied to AI workloads?
How much cooling demand is tied to AI workloads?
How much water demand is tied to AI workloads?
How much heat is produced by AI workloads?
Will AI workloads increase backup power requirements?
Will AI workloads increase hardware replacement and electronic waste?
Can AI-related expansion occur without new public review?
Will AI demand be reported separately where feasible?

Vendor and Secondary Use

Can vendors use data for AI training or product improvement?
Can cloud providers use metadata, prompts, logs, or interactions?

Can public data be used to improve commercial AI products?
Can data be shared with affiliates, subcontractors, researchers, or third parties?
Can data be sold?
Can data be combined with other datasets?
Are secondary uses prohibited unless explicitly approved?
Are violations subject to penalties and contract termination?

Transparency and Accountability

Will AI-related uses be disclosed publicly?
Will public-sector AI systems be listed in a registry?
Will data sources be disclosed?
Will impact assessments be public?
Will audits be independent?
Will affected communities be consulted?
Will Indigenous governments have authority over Indigenous data?
Will the public be notified if AI uses change?
Will approval conditions restrict AI-related expansion or data use?

Red Flags

An AI-related data center proposal deserves greater scrutiny when the public hears:
"This is just infrastructure."
"AI use depends on future tenants."
"The facility is AI-ready."
"Data use is handled by customers."
"The company does not train models on customer data without permission."
"Public-sector AI will follow future regulations."
"Data is de-identified."
"Only metadata is used."
"Facial recognition is not currently planned."
"AI will improve efficiency."
"Security and privacy are built in."
"Details are commercially sensitive."

AI-ready is not neutral.
Customer-controlled is not public accountability.
De-identified is not always safe.
Efficiency is not consent.
Future regulation is not protection today.

What Communities Should Ask For

Before approval, communities should ask for:
An AI-use disclosure statement.

A permitted and prohibited AI-use framework.

A data source and data-use assessment.

A personal data protection plan.

A public-sector data AI-use prohibition unless explicitly approved.

A children's data protection framework.

A health, education, policing, court, immigration, and social service data safeguard plan where relevant.

An Indigenous data sovereignty assessment where Indigenous data may be involved.

A biometric and surveillance prohibition or strict approval framework.

A secondary-use policy.

A vendor data-use restriction.

A public AI registry where public-sector systems are involved.

A public-sector AI impact assessment process.

Independent audits for high-risk AI systems.

Human appeal rights for AI-influenced public decisions.

Data minimization, retention, deletion, and opt-out requirements.

Public reporting of AI-related power, water, cooling, heat, and hardware impacts where feasible.

Clear trigger points requiring new public review if the facility shifts toward AI training, high-density AI workloads, public-sector AI, surveillance AI, or biometric processing.

Legally enforceable penalties for unauthorized AI training, secondary use, data sharing, biometric use, surveillance use, or public-data misuse.

The Public Interest Standard

Not every data center is an AI facility.

But every data center proposed as AI-ready, AI-capable, high-performance, hyperscale, or advanced computing infrastructure should answer the AI questions before approval.

A community should not be asked to approve the physical footprint of artificial intelligence while being told the social, legal, privacy, labour, surveillance, and data questions belong somewhere else.

The AI debate is larger than the data center debate.

But the data center is where AI becomes physical.

And data is where AI becomes powerful.

If governments cannot yet fully regulate the models, they can still regulate access to the data, the use of public records, the exploitation of personal information, the processing of biometric identifiers, the use of children's data, the transfer of Indigenous knowledge, and the conversion of public services into training material for private systems.

AI does not grow from nothing.

It grows from data, electricity, water, land, labour, infrastructure, and permission.

The public has the right to ask whether that permission should be granted.

Addendum B

Questions for Public Hearings

This checklist is designed for public hearings, council meetings, open houses, regulatory reviews, community information sessions, and written submissions.

It is not necessary to ask every question.

Not every question will apply to every project.

The purpose is to help residents, councillors, journalists, farmers, workers, Indigenous governments, local businesses, public agencies, and community organizations identify what has not yet been answered.

A data center proposal should not be judged only by the company's presentation.

It should be judged by the questions the public is allowed to ask — and the answers the public is allowed to verify.

1. What Is Actually Being Proposed?

What kind of data center is this?

Is it cloud storage, colocation, enterprise computing, AI training, AI inference, high-performance computing, crypto mining, government data, surveillance infrastructure, or something else?

Who will own the land?

Who will own the building?

Who will operate the facility?

Who will the tenants be?

Will tenants be publicly disclosed?

What is the total size of the project at full buildout?

How many phases are planned?

Can the facility expand later without new public approval?

What is the expected lifespan of the facility?

What uses are prohibited?

2. Who Benefits?

Who receives the financial benefit from this project?

Is the owner local, national, foreign, private equity, real estate investment, public company, subsidiary, or special-purpose corporation?

Who receives tax incentives or subsidies?

Who receives infrastructure upgrades?

Who receives discounted utilities?

How much permanent local employment will actually result?

How much public revenue will remain after public costs are counted?

What public benefits are legally guaranteed?

3. Public Consultation and Consent

When was the public first notified?

Was the project substantially designed before public consultation began?

Have nearby residents, farmers, Indigenous governments, schools, hospitals, care homes, businesses, and affected communities been directly notified?

Have public materials been written in plain language?

Have technical documents been released?

Has enough time been provided for review?

Will public concerns change the project, or is consultation only informational?

What happens if the public identifies major unanswered risks?

4. Water

How much water will the project withdraw daily, monthly, annually, at peak demand, during drought, and at full buildout?

How much water will be consumed and not returned?

Where will the water come from?

Will it use municipal water, groundwater, surface water, reclaimed water, industrial water, stormwater, or another source?

What happens during drought or water restrictions?

Will the project receive priority water access?

Will water use affect homes, farms, ecosystems, future housing, or public services?

What discharge will be created?

Will discharge temperature and quality be monitored?

Who pays for water infrastructure upgrades?

Will water data be publicly reported in real time or near real time?

5. Electricity and Grid Burden

How much electricity will the project require at first phase and full buildout?

What is the average demand?

What is the peak demand?

Will the project require new substations, transmission lines, transformers, distribution upgrades, or grid reinforcement?

Who pays for those upgrades?

Will costs be passed to ratepayers?

Will the facility receive discounted electricity or special rates?

Will the project increase pressure for new generation?

Will it use fossil power, renewable power, credits, direct supply, or a mix?

Will the facility reduce load during grid emergencies?

Will AI workloads increase future power demand?

6. Land Use and Community Fit

Why was this site chosen?

What alternative sites were considered?

Is the land farmland, wetland, forest, grassland, habitat, floodplain, cultural land, future housing land, or community growth land?

How close is the facility to homes, farms, schools, hospitals, care homes, parks, trails, and public spaces?

How will this site fit the community 10, 20, 30, or 40 years from now?

Will the facility create pressure for more industrial development?

Will future residents be told the facility was there first?

What buffers, setbacks, screening, and land protections are legally required?

7. Sound, Vibration, and Light

What sound will the facility produce during normal operation, night operation, peak cooling, generator testing, construction, maintenance, and emergencies?

Will low-frequency sound be measured?

Will tonal sound be measured?

Will vibration be measured?

Will sound be measured at homes, farms, barns, schools, care facilities, wildlife areas, and future residential areas — or only at the property line?

Will monitoring be continuous?

Will the data be public?

What limits apply at night?

How will light trespass be prevented?

Will lighting affect wildlife, livestock, neighbours, night sky, or nearby roads?

What happens if residents experience noise or light impacts despite technical compliance?

8. Heat and Cooling

What cooling system will be used?

How much heat will the facility produce?

Where will that heat go?

Could the project worsen local heat island effects?

Will cooling demand increase during heat waves?

Will the facility use more water or power during extreme heat?

Has waste heat recovery been studied?

Could waste heat be used for public buildings, schools, hospitals, recreation centres, greenhouses, social housing, shelters, or district heating?

If waste heat is not used, why not?

9. Air, Emissions, and Backup Power

Will diesel generators, gas turbines, batteries, or other backup systems be used?

How many generators will there be?

How much fuel will be stored on site?

How often will generators be tested?

What emissions will generator testing create?

What happens during long grid outages?

Will generator emissions be monitored and publicly reported?

Will batteries create fire or chemical risks?

What refrigerants, coolants, chemicals, oils, or fire suppression substances will be used?

Could emissions, smoke, spills, or chemical releases affect nearby homes, farms, schools, care facilities, waterways, or wildlife?

10. Wildlife, Livestock, Crops, and Ecosystems

What plants, animals, wetlands, waterways, soils, farms, and habitats may be affected?

Have livestock impacts been studied?

Have crop, soil, and drainage impacts been studied?

Have pollinators, birds, bats, amphibians, aquatic life, and wildlife corridors been assessed?

Will noise, vibration, light, heat, traffic, construction, runoff, or fencing affect animals or ecosystems?

Will habitat be fragmented?

What restoration is required?

Who monitors ecological impacts after approval?

What happens if impacts are worse than predicted?

11. Cumulative Impacts

Is this project being assessed alone, or as part of a larger pattern?

Are other data centers proposed, approved, or likely nearby?

Will the infrastructure built for this project enable more data centers?

What happens if several facilities use the same water system, grid, roads, emergency services, or watershed?

Has full regional buildout been assessed?

Will cumulative water, power, noise, heat, emissions, land, habitat, traffic, and public-cost impacts be reviewed?

What limits will prevent uncontrolled clustering?

12. Data Sovereignty, Privacy, and Surveillance

Will public-sector data be stored or processed here?

Will health, education, policing, court, immigration, correctional, social service, utility, or municipal data be involved?

Will personal data be used for AI training, analytics, profiling, or automated decisions?

Will the facility support facial recognition, smart-city surveillance, licence plate readers, predictive policing, immigration enforcement, or public-sector AI?

Who controls the data?

Can foreign governments, courts, intelligence agencies, or parent-company jurisdictions access the data?

Where will backups be stored?

Who controls encryption keys?

Can data be moved outside the country?

Can people see, correct, delete, or challenge use of their data?

13. Ownership and Corporate Structure

Who is the real beneficial owner?

Is the applicant a subsidiary, numbered company, shell company, special-purpose vehicle, real estate trust, private equity vehicle, or local affiliate?

Who owns the parent company?

Who owns the land, building, servers, and operating company?

Who receives subsidies?

Who is liable if something goes wrong?

Do parent-company guarantees exist?

What happens if the project is sold, transferred, restructured, or goes bankrupt?

Do all obligations survive ownership changes?

14. Jobs and Economic Claims

How many construction jobs will be created?

How many permanent jobs will remain five years after opening?

How many permanent jobs will be local?

What wages and benefits will be paid?

Will jobs be union, full-time, part-time, contract, remote, or temporary?

Will local training be funded?

Will Indigenous hiring be included where appropriate?

Will local procurement be required?

What is the public cost per permanent local job?

Are job promises legally enforceable?

What happens if they are not met?

15. Taxes, Subsidies, and Public Costs

What tax breaks are being requested?
What sales tax, property tax, equipment tax, or other exemptions are involved?
Will electricity or water be discounted?
Will grants, loans, loan guarantees, land discounts, or infrastructure funding be provided?
What is the total public subsidy from all levels of government and utilities?
What public revenue is being forgone?
What public costs are being assumed?
Are all subsidy agreements public?
Do clawbacks exist?
Can tax benefits be revoked if promises are broken?

16. Infrastructure and Ratepayer Burden

What infrastructure must be built or upgraded?
Who pays for substations, transmission lines, water pipes, sewer upgrades, stormwater systems, roads, bridges, fire capacity, emergency equipment, and grid reinforcement?
Will taxpayers pay?
Will ratepayers pay?
Will costs be hidden in utility bills?
Will maintenance costs fall to the public?
Are upgrades sized for this project or future expansion?
Will infrastructure built for the data center reduce capacity for housing, farms, public services, or local businesses?
Has a full taxpayer and ratepayer impact assessment been released?

17. Emergency Planning

What emergencies are possible?
Does the plan include fire, explosion, battery failure, diesel spill, chemical release, water contamination, cyberattack, grid failure, cooling failure, extreme heat, flood, wildfire, evacuation, and severe weather?
Can local emergency services handle the facility?
Will fire departments need new training, equipment, water supply, or staffing?
Who pays for emergency preparedness?
How will the public be notified during an incident?
Can contaminated runoff be contained on site?
Will emergency plans be public enough for residents to understand their risk?
Have emergency drills been completed before operation begins?

18. Monitoring and Public Reporting

What will be monitored after approval?
Water use?

Power use?
Noise?
Vibration?
Light?
Emissions?
Generator testing?
Heat?
Discharge?
Wildlife?
Livestock?
Traffic?
Outages?
Complaints?
Will monitoring begin before construction to establish baseline conditions?
Will data be real time, near real time, monthly, annual, or only company summary?
Will raw data be public?
Who owns the monitors?
Who audits the data?
What happens if monitoring equipment fails?
Will public complaints be logged, investigated, mapped, and publicly reported?

19. Enforcement and Public Remedies

What happens if the company breaks a condition?
Can permits be suspended?
Can operations be restricted?
Can water use be reduced?
Can power demand be capped?
Can generator testing be limited?
Can tax benefits be revoked?
Can subsidies be clawed back?
Can fines escalate?
Can future phases be denied?
Can the public trigger review?
Can residents, farmers, Indigenous governments, municipalities, or public agencies seek remedies?
Are penalties large enough to matter?
Who enforces each condition?

20. Decommissioning and Exit Plans

What happens when equipment ages?
What happens if tenants leave?

What happens if the company sells?
What happens if the facility becomes obsolete?
What happens if the project is abandoned?
Is there a decommissioning plan?
Is there a cleanup plan?
Is there a data deletion and data transfer plan?
Is there a bond, reserve fund, letter of credit, insurance, or parent-company guarantee?
Who removes servers, batteries, generators, fuel tanks, chemicals, cooling systems, and electronic waste?
Who pays if the company no longer exists?

21. Community Benefits

Will there be a legally binding Community Benefit Agreement?
What local hiring is guaranteed?
What training is guaranteed?
What Indigenous hiring or procurement is included where appropriate?
What public broadband improvements are guaranteed?
Will waste heat be used for district heating, public buildings, greenhouses, or community energy?
Will water offsets be local, measurable, and enforceable?
Will environmental restoration be required?
Will emergency service funding be provided?
Will public reporting be required?
What happens if community benefits are not delivered?

Final Public Hearing Questions

Before approval, ask:
What information is still missing?
Which promises are legally binding?
Which promises are voluntary?
Which documents are public?
Which documents are confidential?
Who pays if projections are wrong?
Who benefits if the project succeeds?
Who carries the burden if it fails?
What happens if impacts are worse than predicted?
What happens if the company changes owners, tenants, or uses?
What power does the public have after approval?

A Closing Statement for Public Hearings

I am not asking whether data centers should exist.

I am asking whether this data center, in this location, at this scale, with these water demands, power demands, infrastructure costs, public subsidies, environmental impacts, data risks, emergency risks, and community obligations, has been fully understood before approval.

If the answer is yes, the evidence should be public.

If the answer is no, approval should wait.

Addendum C

Documents to Request

A data center proposal should not be evaluated only from slide decks, public-relations summaries, council presentations, or economic development announcements.

The real answers are usually in the documents.

Power agreements.

Water licences.

Grid studies.

Traffic studies.

Acoustic reports.

Environmental assessments.

Tax agreements.

Emergency plans.

Ownership disclosures.

Subsidy documents.

Infrastructure cost estimates.

Monitoring plans.

Community benefit agreements.

Some documents may be held by municipalities. Others may be held by utilities, regulators, water authorities, provincial or state agencies, federal departments, economic development offices, planning departments, emergency services, or the developer itself.

This addendum is a checklist of documents residents, councillors, journalists, Indigenous governments, local organizations, farmers, workers, and public agencies can request.

Not every document will exist for every project.

That is also useful information.

If a document does not exist, the public should ask why.

1. Project Description and Application Documents

Request:
The full development application.
The full planning application.
The rezoning application.
The land-use amendment application.
The site plan.
The master plan.
The phasing plan.
The full-buildout plan.
The project description submitted to regulators.
The construction timeline.
The operations description.
The tenant-use description.
The list of proposed and prohibited uses.
The building height, footprint, floor area, rack density, and total campus size.
The design drawings and renderings.
The landscaping, buffering, screening, and lighting plans.
The drainage and grading plans.
The public consultation record.
The developer's response to public concerns.
Ask whether the project being shown to the public is the first phase only or the full development.

2. Ownership and Corporate Structure

Request:
The beneficial ownership disclosure.
The corporate ownership chart.
The applicant's corporate registration.
Parent-company information.
Subsidiary and affiliate information.
Special-purpose vehicle information.
Landowner disclosure.
Building owner disclosure.
Operator disclosure.
Tenant disclosure where available.
Investor disclosure where available.
Real estate investment trust or private equity involvement where applicable.
Foreign ownership or control disclosure.

Corporate restructuring or sale provisions.
Parent-company guarantees.
Liability and indemnity agreements.
Insurance certificates.

Ask who owns the land, who owns the building, who owns the servers, who operates the facility, who receives public benefits, and who remains liable if something goes wrong.

3. Power, Grid, and Electricity Documents

Request:
Power supply agreements.
Electricity service agreements.
Grid connection applications.
Interconnection studies.
Load studies.
Transmission studies.
Distribution studies.
Substation plans.
Transformer plans.
Switchyard plans.
Grid reinforcement studies.
Peak load projections.
Average load projections.
Full-buildout load projections.
Power demand by phase.
Backup power plans.
Generator specifications.
Battery storage plans.
Renewable energy agreements.
Power purchase agreements.
Special electricity rate agreements.
Utility tariff agreements.
Curtailment agreements.
Demand-response agreements.
Grid reliability assessments.
Ratepayer impact assessments.

Ask who pays for substations, transmission lines, distribution upgrades, transformers, grid reinforcement, and any new generation or reserve capacity required by the project.

4. Water Documents

Request:
Water licence applications.

Water licences.
Water withdrawal permits.
Water allocation agreements.
Municipal water service agreements.
Groundwater studies.
Aquifer studies.
Surface water studies.
Watershed assessments.
Water balance reports.
Cooling water demand estimates.
Peak water demand estimates.
Seasonal water demand estimates.
Drought-period water demand estimates.
Full-buildout water demand estimates.
Construction water demand estimates.
Reclaimed water agreements.
Industrial water agreements.
Stormwater reuse plans.
Water conservation plans.
Water offset plans.
Water infrastructure capacity studies.
Water rate agreements.
Water monitoring plans.

Ask how much water will be withdrawn, how much will be consumed, how much will be discharged, where it comes from, what happens during drought, and who pays for infrastructure upgrades.

5. Wastewater, Sewer, and Discharge Documents

Request:
Wastewater discharge permits.
Sewer service agreements.
Sewer capacity studies.
Wastewater treatment capacity assessments.
Industrial discharge permits.
Thermal discharge studies.
Discharge temperature limits.
Water quality monitoring plans.
Chemical discharge inventories.
Cooling system blowdown reports.
Stormwater management plans.
Stormwater pond designs.

Runoff containment plans.
Emergency shutoff plans.
Spill response plans.
Downstream impact assessments.

Ask whether the facility will discharge heat, chemicals, treated water, contaminated runoff, or stormwater into public systems, waterways, wetlands, ditches, groundwater, or neighbouring land.

6. Environmental Assessment Documents

Request:
Environmental impact assessments.
Environmental screening reports.
Cumulative impact assessments.
Climate impact assessments.
Greenhouse gas assessments.
Air quality assessments.
Water impact assessments.
Wetland assessments.
Wildlife surveys.
Habitat assessments.
Species-at-risk assessments.
Bird and bat studies.
Pollinator studies.
Aquatic life assessments.
Soil studies.
Agricultural impact assessments.
Livestock impact assessments.
Vegetation studies.
Tree removal plans.
Habitat restoration plans.
Environmental mitigation plans.
Environmental monitoring plans.
Environmental compliance reports.

Ask whether the assessment looks only at the project boundary or also at the watershed, airshed, wildlife corridors, farms, neighbouring properties, and full-buildout impacts.

7. Sound, Vibration, and Light Documents

Request:
Acoustic impact assessments.
Noise modelling reports.
Low-frequency sound studies.
Tonal sound assessments.

Nighttime sound studies.
Vibration studies.
Construction noise plans.
Generator testing noise assessments.
Transformer noise assessments.
Cooling equipment sound specifications.
Sound mitigation plans.
Noise monitoring plans.
Measurement location maps.
Baseline sound studies.
Complaint response procedures.
Lighting plans.
Light trespass assessments.
Dark-sky assessments.
Wildlife lighting assessments.

Ask whether sound will be measured only at the property line or also at homes, farms, barns, schools, care facilities, wildlife areas, public spaces, and future residential areas.

8. Heat and Cooling Documents

Request:
Cooling system design documents.
Cooling technology alternatives assessment.
Heat rejection estimates.
Heat island assessments.
Extreme heat operation plans.
Cooling failure plans.
Thermal discharge studies.
Waste heat recovery studies.
District heating feasibility studies.
Heat reuse agreements.
Greenhouse heating feasibility studies.
Public facility heating assessments.
Cooling water use estimates.
Cooling power demand estimates.
Refrigerant inventories.
Coolant inventories.
Cooling chemical inventories.

Ask whether waste heat can be used for public buildings, district heating, greenhouses, social housing, recreation centres, hospitals, schools, shelters, or other community uses.

9. Air, Emissions, and Backup System Documents

Request:
Air quality assessments.
Emissions inventories.
Generator specifications.
Generator testing schedules.
Generator runtime estimates.
Diesel fuel storage plans.
Gas turbine plans where applicable.
Fuel delivery plans.
Fuel spill response plans.
Fuel tank permits.
Battery storage specifications.
Battery fire risk assessments.
Thermal runaway assessments.
Fire suppression system details.
Refrigerant and coolant inventories.
Hazardous material inventories.
Greenhouse gas assessments.
Construction emissions plans.
Dust control plans.
Air monitoring plans.
Emergency generator reporting plans.
Ask what emissions occur during normal operation, generator testing, grid outages, emergencies, construction, and full buildout.

10. Traffic, Roads, and Transportation Documents

Request:
Traffic impact studies.
Construction traffic plans.
Heavy-haul route plans.
Oversized load permits.
Road widening plans.
Intersection upgrade plans.
Bridge capacity assessments.
Culvert and drainage assessments.
Access road plans.
Emergency access plans.
Parking plans.
Worker transportation plans.
Fuel delivery route plans.

Equipment delivery route plans.
Road maintenance agreements.
Road damage repair agreements.
Transportation mitigation plans.
Ask who pays for road widening, bridge strengthening, traffic signals, turning lanes, road repairs, and long-term maintenance.

11. Infrastructure Cost and Ratepayer Documents

Request:
Infrastructure cost assessments.
Direct cost estimates.
Indirect cost estimates.
Full-buildout servicing studies.
Off-site infrastructure studies.
Development charge calculations.
Impact fee calculations.
Servicing agreements.
Utility cost-recovery agreements.
Ratepayer impact assessments.
Taxpayer impact assessments.
Municipal capital budget impacts.
Water rate impact studies.
Sewer rate impact studies.
Electricity rate impact studies.
Stormwater rate impact studies.
Maintenance cost estimates.
Lifecycle cost assessments.
Ask whether costs are being paid by the developer, taxpayers, utility customers, future residents, or other public budgets.

12. Tax, Subsidy, and Incentive Documents

Request:
Tax incentive agreements.
Property tax abatement agreements.
Sales tax exemption documents.
Equipment tax exemption documents.
Payment-in-lieu agreements.
Special assessment agreements.
Tax freeze agreements.
Grant agreements.
Loan agreements.

Loan guarantee agreements.
Low-interest financing documents.
Land discount agreements.
Infrastructure funding agreements.
Workforce subsidy agreements.
Economic development agreements.
Utility discount agreements.
Public subsidy summaries.
Cost-benefit analyses.
Public return on investment assessments.
Clawback provisions.

Ask what the project would pay without incentives, what it will actually pay, how long the incentives last, and whether benefits can be recovered if promises are broken.

13. Jobs and Economic Development Documents

Request:
Economic impact assessments.
Job creation estimates.
Construction job estimates.
Permanent job estimates.
Local hiring plans.
Workforce training plans.
Apprenticeship plans.
Wage and benefit commitments.
Union or labour agreements where applicable.
Local procurement plans.
Indigenous hiring and procurement plans where applicable.
Small business participation plans.
Workforce housing assessments.
Public cost-per-job calculations.
Independent verification of economic claims.

Ask how many permanent local full-time jobs will exist five years after opening and what the public cost is per job.

14. Emergency Planning Documents

Request:
Emergency response plans.
Fire response plans.
Explosion risk assessments.
Battery failure response plans.
Thermal runaway response plans.

Diesel spill response plans.
Chemical release response plans.
Water contamination response plans.
Cyber incident response plans.
Grid failure response plans.
Cooling failure response plans.
Extreme heat response plans.
Flood response plans.
Wildfire response plans.
Severe weather response plans.
Evacuation plans.
Shelter-in-place plans.
Public alert and notification plans.
Fire department capacity assessments.
Emergency medical services assessments.
Police and security coordination plans.
Hazardous-material response plans.
Mutual aid agreements.
Emergency drill schedules.
After-action reporting requirements.

Ask whether local emergency services have the equipment, training, staffing, water supply, access, and funding required to respond.

15. Cybersecurity, Privacy, Public Data, and AI Documents

Request:
Cybersecurity risk assessments.
Critical infrastructure assessments.
Public-sector data assessments.
Privacy impact assessments.
Surveillance impact assessments.
AI impact assessments.
Automated decision-system assessments.
Data sovereignty assessments.
Data residency documents.
Data transfer agreements.
Data-sharing agreements.
Encryption and key-control policies.
Vendor data access agreements.
Cloud service agreements involving public data.
Public-sector AI use policies.
Biometric data policies.

Facial recognition policies.
Data retention and deletion schedules.
Breach notification plans.
Public data exit plans.
Indigenous data governance assessments where applicable.
Children's data protection assessments where applicable.
Ask whether public data, personal data, health data, school data, policing data, immigration data, biometric data, or Indigenous data can be used for AI, analytics, profiling, surveillance, or secondary purposes.

16. Monitoring, Reporting, and Enforcement Documents

Request:
Monitoring plans.
Baseline monitoring reports.
Water monitoring plans.
Power monitoring plans.
Emissions monitoring plans.
Noise monitoring plans.
Vibration monitoring plans.
Light monitoring plans.
Heat monitoring plans.
Wildlife monitoring plans.
Livestock monitoring plans.
Soil and crop monitoring plans.
Complaint response procedures.
Public dashboard plans.
Raw data access policies.
Independent audit requirements.
Compliance reporting requirements.
Inspection protocols.
Enforcement plans.
Penalty schedules.
Permit condition tables.
Public trigger provisions.
Corrective action plans.
Ask whether data will be available in real time or near real time, or only through company summaries.

17. Conditions, Clawbacks, and Public Remedies Documents

Request:
Draft approval conditions.

Final approval conditions.
Development agreements.
Operating agreements.
Permit conditions.
Water-use conditions.
Power-demand conditions.
Noise limits.
Emissions limits.
Generator testing restrictions.
Lighting conditions.
Traffic conditions.
Environmental mitigation conditions.
Public reporting conditions.
Clawback provisions.
Penalty schedules.
Permit suspension powers.
Future phase review requirements.
Public complaint escalation procedures.
Public trigger rights.
Legal remedies for residents, farmers, Indigenous governments, municipalities, public agencies, and ratepayers.
Ask which promises are legally binding and what happens if they are broken.

18. Community Benefit Agreement Documents

Request:
Draft Community Benefit Agreement.
Final Community Benefit Agreement.
Local hiring commitments.
Training commitments.
Apprenticeship commitments.
Indigenous benefit agreements where applicable.
Local procurement commitments.
Public broadband commitments.
Waste heat recovery commitments.
District heating agreements.
Water offset commitments.
Environmental restoration commitments.
Emergency service funding commitments.
Public reporting commitments.
Community oversight committee terms.
Independent audit provisions.

Enforcement provisions.
Ask whether community benefits are legally enforceable or merely voluntary.

19. Decommissioning and Exit Documents

Request:
Decommissioning plans.
Closure plans.
Equipment removal plans.
Electronic waste management plans.
Battery recycling plans.
Generator removal plans.
Fuel tank removal plans.
Refrigerant and coolant recovery plans.
Chemical disposal plans.
Environmental cleanup plans.
Soil and groundwater testing plans.
Site restoration plans.
Data transfer and deletion plans.
Public-sector continuity plans.
Stranded infrastructure assessments.
Decommissioning cost estimates.
Bonds.
Reserve funds.
Letters of credit.
Insurance policies.
Parent-company guarantees.
Ask who pays if the facility becomes obsolete, tenants leave, the company sells, or the project is abandoned.

20. Indigenous Rights, Consultation, and Governance Documents

Request where applicable:
Consultation records.
Duty-to-consult assessments.
Indigenous government correspondence.
Traditional land-use studies.
Cultural impact assessments.
Treaty rights assessments.
Harvesting impact assessments.
Water rights assessments.
Indigenous data sovereignty assessments.
Indigenous environmental monitoring agreements.

Indigenous benefit agreements where rights-holders choose them.

Accommodation measures.

Dispute resolution processes.

Ask whether Indigenous governments were involved early enough to influence the project, not merely notified after key decisions were made.

21. Public Communication Documents

Request:

Public notice records.

Open house materials.

Presentation slides.

Question-and-answer records.

Technical summaries.

Plain-language project summaries.

Public comment submissions.

Developer responses to public comments.

Council briefing notes.

Staff reports.

Regulator correspondence.

Meeting minutes.

Consultant reports.

Public engagement plans.

Communications strategies.

Ask whether the public received the same information decision-makers received.

If Documents Are Withheld

If a document is withheld, ask:

Who has the document?

Why is it being withheld?

Is the reason legal, commercial, security-related, privacy-related, or political?

Can a redacted version be released?

Can a summary be released?

Can the public authority review the unredacted document?

Can councillors or regulators review it confidentially?

Can an independent expert review it?

Can approval proceed without public access to the information?

A project should not be approved because the most important information is hidden.

Public Records Request Template

Use or adapt the following wording:

I am requesting copies of all documents, studies, agreements, reports, permits, correspondence, technical assessments, staff reports, consultant reports, and approval conditions related to the

proposed data center project, including but not limited to power agreements, grid studies, water licences, water service agreements, environmental assessments, traffic studies, acoustic reports, emergency plans, ownership disclosures, tax incentive agreements, subsidy agreements, infrastructure cost assessments, ratepayer impact assessments, monitoring plans, enforcement provisions, and Community Benefit Agreements.

Please include draft versions, final versions, attachments, appendices, maps, modelling files, consultant reports, public presentations, staff briefings, and correspondence with the applicant, utilities, regulators, other levels of government, and affected agencies.

If any records are withheld, please identify the record, the reason for withholding it, and whether a redacted version can be released.

The Public Interest Standard

No community should be asked to approve a data center without access to the documents needed to understand it.

A slide deck is not disclosure.

A press release is not evidence.

A summary is not the record.

If the project requires public land-use approval, public infrastructure, public water, public grid capacity, public emergency services, public subsidies, or public tolerance, then the public has the right to see the documents behind the proposal.

The question is simple:

What have decision-makers seen that the public has not?